

Version 10.2











GroupID Reports

GroupID Insights

User Guide Authenticate

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

© 2022 Imanami | Now Part of Netwrix. Trademarks are the property of their respective owners.

Contents

Chapter 1 - About GroupID Authenticate1
Launch GroupID Authenticate
Enable Integrated Windows Authentication
GroupID Security Service5
Part 1 - GroupID as a Service Provider1
Chapter 1 - SAML Configuration for GroupID using AD FS
Generate Consumer URL3
Generate Entity ID/Audience URL4
Configure relaying party trust in AD FS
Specify claim rules for authentication
Configure the AD FS provider in GroupID14
Provide Issuer URL15
Provide IDP Login URL16
Upload image for identity provider
Get token-signing certificate17
Advanced configurations 21
Sign-in using AD FS 24
Chapter 2 - SAML Configuration for GroupID using Azure AD SSO27
Generate Consumer URL 27
Generate Entity ID/Audience URL
Configure GroupID in Azure AD for SSO
SAML SSO configurations for the application33
Configure the Azure AD SSO application in GroupID
Sign in using Azure AD SSO
Chapter 3 - SAML Configuration for GroupID using Okta
Generate Consumer URL
Generate Entity ID/Audience URL

Configure GroupID in Okta	.41
Download Okta metadata file	.47
Configure users in Okta	.48
Configure the Okta provider in GroupID	.51
Sign-in using Okta	.53
Chapter 4 - SAML Configuration for GroupID us PingOne	-
Generate GroupID metadata file	.56
Generate Consumer URL	.56
Download metadata file	.57
Configure GroupID in PingOne	.58
Attribute mapping in PingOne	.62
Configure the PingOne provider in GroupID	.64
Configure users in PingOne	.67
Sign-in using PingOne	.68
Sign-in using PingOne Chapter 5 - SAML Configuration for GroupID us OneLogin	ing
Chapter 5 - SAML Configuration for GroupID us	ing 70
Chapter 5 - SAML Configuration for GroupID us OneLogin	ing 70 .70
Chapter 5 - SAML Configuration for GroupID us OneLogin	ing 70 .70 .71
Chapter 5 - SAML Configuration for GroupID us OneLogin Generate Consumer URL Generate Entity ID/Audience URL	ing 70 .70 .71 .71
Chapter 5 - SAML Configuration for GroupID us OneLogin Generate Consumer URL Generate Entity ID/Audience URL Configure GroupID in OneLogin	ing 70 .70 .71 .71 .77
Chapter 5 - SAML Configuration for GroupID us OneLogin Generate Consumer URL Generate Entity ID/Audience URL Configure GroupID in OneLogin Configure the OneLogin provider in GroupID	ing 70 .70 .71 .71 .77 .80
Chapter 5 - SAML Configuration for GroupID us OneLogin	ing 70 .70 .71 .71 .77 .80 .84
Chapter 5 - SAML Configuration for GroupID us OneLogin Generate Consumer URL Generate Entity ID/Audience URL Configure GroupID in OneLogin Configure the OneLogin provider in GroupID Define users in OneLogin Sign-in using OneLogin	ing 70 .70 .71 .71 .77 .80 .84 .84 .86
Chapter 5 - SAML Configuration for GroupID us OneLogin	ing 70 .70 .71 .71 .77 .80 .84 86 87
Chapter 5 - SAML Configuration for GroupID us OneLogin	ing 70 .70 .71 .71 .77 .80 .84 86 87 .87
Chapter 5 - SAML Configuration for GroupID us OneLogin	ing 70 .70 .71 .71 .77 .80 .84 86 87 .87 .90

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:

- <u>AD FS</u>
- <u>Azure AD SSO</u>
- <u>Okta</u>
- <u>PingOne</u>
- 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.

• 🔿 📶 🖬 🖬						
Corrupti (Loc) Automate Self-Service Mobile Service Mobile Service Mobile Service Password Center Scheduling Configuration Repictations Reports Reports Reports Reports Notifications	Identity Provi	iden identity Store Local	Olent Automate DEV	Status Enabled	Actions Authenticate Admin Panel O User Enrollment Vrew Vrew Help	

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.

Windows Security	×
iexplore	
Connecting to win2k16-ex16.je	e.local.
A User name	
Password	
Domain: JEE	
Remember my cr	edentials
ОК	Cancel

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:

GroupID							
((•)) SAML Providers	Applications	Generate URL's	Authentication Settings				
Welcome Adminis	trator,	D ₂					
SAML Identity Provid	lers						
+ New Provider							
Name	Issue:			Client	Display On Login Page:	Actions	
ADFS	https://SAMSUNG-DC.askari.l	ocal/adfs/services/trust		SR1	Yes	B 🔒	Evalued

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	

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:

Š			Registry Editor	_
File Edit View Favorites Help				
⊿ 👰 Computer	Name	Туре	Data	
HKEY_CLASSES_ROOT	ab (Default)	REG_SZ	(value not set)	
⊿ - → HKEY_CURRENT_USER	ab AuthNegotiateDelegateWhitelist	REG_SZ	MYIISSERVER	
AppEvents	ab AuthSchemes	REG_SZ	basic, digest, ntlm, negotiate	
Console	ab AuthServerWhitelist	REG_SZ	MYIISSERVER	
D Control Panel		100_02	in hose the h	
EUDC				
Keyboard Layout				
Printers				
⊿ - 🔐 Software				
AppDataLow				
AvastAdSDK				
D Classes				
þ 🍶 Google				
þ 🍶 Imanami				
JavaSoft				
Microsoft				
Mozilla				
Piriform				
A Dolicies				
a 🚹 Google				
Chrome				
Microsoft				
Dower				

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**.

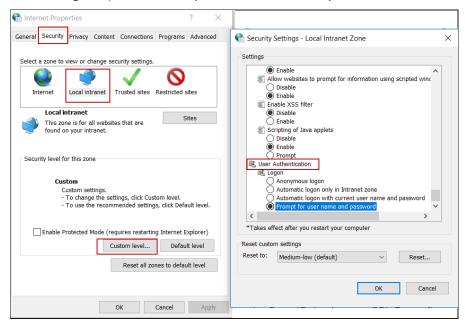


Figure 5: Settings for Internet Options

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.

((+)) SAML Providers 🗈 Applicat	tions 💮 Generate URL's	2 Authentication Settings	
Welcome gid1,			
Generate URL's			
Consumer URL			
Select client to generate consumer URL		Consumer URL	
Automate WIN-GID9SERVER	~	https://win-gid9servers443/GroupID5ecurtyService/Sami/6656601c-a47a-4850-8117-e377329efc57	
Login URL			
Select Identity Provider to Generate Log	gin URL:	Login URL	
	~		
Metadata			
nin La Galla			
identity store:		Client GroupID Metadata URL:	
Cheoti	~	Automata WIN-GIDSERVER V https://win-gidServer/443/GroupIDSecurityService/samilimetadetaltcler	0

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*.

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.



 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.
 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.

((•)) SAML Providers Applications	💮 Generate	URL'S 🔯 Authentication Settings					
Create New Provider							
Basic							
Name:		Issueri		IDP Certificate:			
IDP Login URL:		Status: Enabled	~				
lidentity store:		Client:		Entity ID/Audience:			
Cheosi Identity Provider Image:	~	Automate WIN-GID0SERVER	~	https://win-gid9server/GroupIDSecurityService/1/A			
No Image Selected							
Advanced							~
					Import from Metadata	Cancel	Create 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

 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.

🏟 File Action Viev					
🔛 AD FS		Relying Party Trusts			Actions
A PD P3 Service A Service Children Children Children Children Certificates Calim Decroit Children Ch	ps der Trusts Add Relying Party	Display Name En Device Registration Service Ye GroupID Ye		Identifier um me der adfa gid 8 loc https://gid8.4443/GroupIDSecuritySe	Relying Party Trusts Add Reying Party Trust Add Non-Claims-Aware Relying Party Trust View New Window from Here C Refresh I I Hep
	New Window from Refresh Help	n Here			GroupID Update from Federation Metadata Edit Claim Rules Disable Properties Properties Delete 2 Help

Figure 8: AD FS Console

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

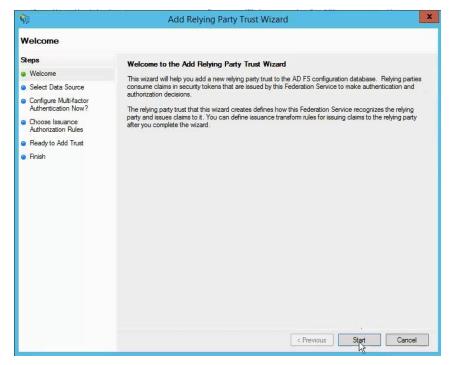


Figure 9: Welcome page

3. Read the welcome message and click Start.

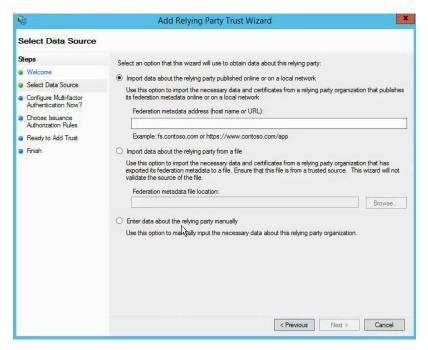


Figure 10: Select Data Source page

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**.

Ŵ	Add Relying Party Trust Wizard	x
Specify Display Nan	ne	
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source		
Specify Display Name	Notes:	
Choose Profile		~
Configure Certificate		
Configure URL		
Configure Identifiers		
Configure Multi-factor Authentication Now?		×
 Choose Issuance Authorization Rules 		
Ready to Add Trust		
 Finish 		
	< Previous Next > Cancel	
		-

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.

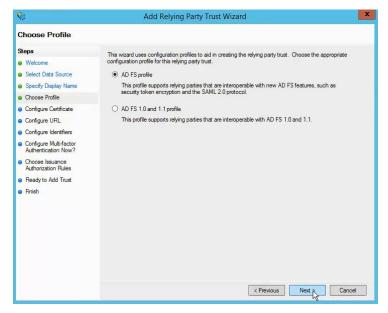


Figure 12: Choose Profile page

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

\$	Add Relying Party Trust Wizard	X
Configure Certificat	3	
Configure Certificat Steps • Welcome • Select Data Source • Specify Display Name • Configure Orbita • Configure VIRL • Configure URL • Configure Identifiens • Configure Multi-factor Authentication Now? • Choose Issuance Authoritication Rules • Ready to Add Trust • Finish	Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the clams that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the clams that are sent to it. To specify the certificate, click Browse. Issuer: Subject: Subject: Effective date: Expiration date: New Wew Browse	
	< Previous Next > Cancel	

Figure 13: Configure Certificate page

9. Click Next.

\$	Add Relying Party Trust Wizard
Configure URL	
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Multi-factor Authentication Now? Ready to Add Trust Finish	AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Federation Passive protocol The WS-Federation Passive protocol The WS-Federation Passive protocol Relying party WS-Federation Passive protocol Relying party WS-Federation Passive protocol Relying party WS-Federation Passive protocol URL: Example: https://fs.contoso.com/adfs/s/ Enable support for the SAML 2.0 WebSSO protocol The SAML 2.0 studie-sign-on (SSO) service URL: WS-Federation Passive protocol. Relying party SAML 2.0 SSO service URL: Example: https://sAML 2.0 SSO service URL: Example: https://www.contoss.com/adfs/ls/
	< Previous Next > Cancel

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.

Ŷ	Add Relying Party Trust Wizard
Configure Identifiers	
Configure Identifiers Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure URL Configure URL Configure Multi-factor Atthentication Now? Confose Issuance Atthonation Rules Ready to Add Trust Finish	Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust. Relying party trust identifier: Image: Add image: Integration of the image is a string of th
	< Previous Next > Cancel

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**.

V a	Add Relying Party Trust Wizard
Steps Welcome Select Data Source	Configure multifactor authentication settings for this relying party trust. Multifactor authentication is required if there is a match for any of the specified requirements.
Specify Display Name	Multi-factor Authentication Global Settings
 Choose Profile Configure Certificate 	Requirements Users/Groups Not configured Device Not configured
Configure URL	
Configure Identifiers	Location Not configured
Configure Multi-factor Authentication Now?	
 Choose Issuance Authorization Rules 	
 Ready to Add Trust Finish 	I do not want to configure multi-factor authentication settings for this relying party trust at this time. Configure multi-factor authentication settings for this relying party trust. You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see <u>Configuring Authentication Policies</u> .
	< Previous Net > Cancel

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**.

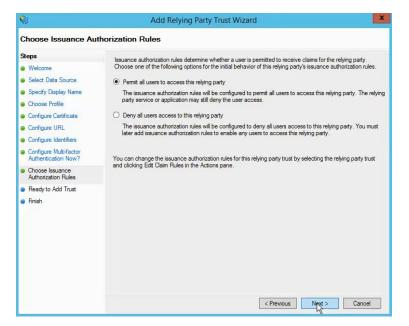


Figure 17: Choose Issuance Authorization Rules page

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**.

\$ 10	Add Relying Party Trust Wizard
Ready to Add Trust	
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure URL Configure Multifactor Authentication New? Choose Issuance Authonzation Neules Ready to Add Trust Finish	The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database. Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Note < > Specify the monitoring settings for this relying party trust. Relying party's federation metadata URL: Automatically update relying party This relying party Sederation metadata data was last checked on: <never> This relying party was last updated from federation metadata on: <never></never></never>
	< Previous Next Cancel

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**.

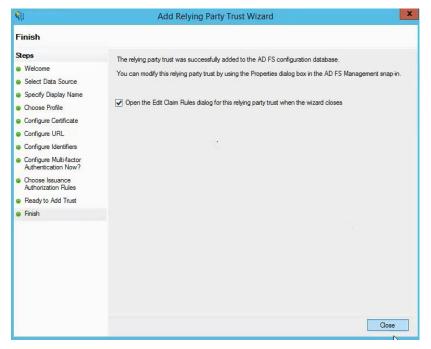


Figure 19: Finish page

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

ssuance Transform Rules	Issuance Authorization Rules		lules
The following transform n	les specify the claims that will l	be sent to the relying party.	
Order Rule Name		Issued Claims	
			1
Add Rule Edit F	Rule		
	OH	(Cancel	Apply

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**.

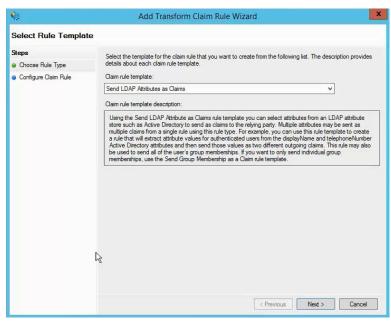


Figure 21: Choose Rule Type page

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

Configure Rule							
Steps Ohoose Rule Type	also map an incoming claim	o map an incoming claim type to an outgoing claim type. As an option, you value to an outgoing claim value. Specify the incoming claim type to map the the decident of the second se					
Configure Claim Rule	Claim rule name:	outgoing claim type and whether the claim value should be mapped to a new claim value.					
	U						
	Rule template: Transform an	Incoming Claim					
	Incoming claim type:	Specify Claim Type 🗸					
	Incoming name ID format:	Unspecified 🗸					
	Outgoing claim type:	Specify Claim Type 🗸					
	Outgoing name ID format:	Unspecified					
	Pass through all claim val	lues					
	Replace an incoming clair	m value with a different outgoing claim value					
	Incoming claim value:						
	Outgoing claim value:	Browse					
	O Replace incoming e-mail	suffix claims with a new e-mail suffix					
	New e-mail suffix:						
		Example: fabrikam.com					

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.

- 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.

The follo		Issuance Authorization Ru	at will be pe	~	14
party. W Order	hen the list does Rule Name	not contain a rule, all users	will be den		
1	Permit Access	to All Users	Permit		
				Γ	^
					•
Add F	lule	Rule Remove Rule			

Figure 23: Issuance Authorization Rules tab

The issuance authorization rule is already completed.

	ers to the relying	on rules specify the users that v party. When the list does not c		
Order	Rule Name		Issued Claims	
				÷
Add F	Rule Edit F	Rule Remove Rule		

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.

reate New Provider					
Basic					
Name:		Issuer:		IDP Certificate:	
IDP Login URL:		Status: Enabled	~		
Identity Store :		Client:		Entity ID/Audience:	
Heaven	~	Automate ASAD-DEV-VM	~	https://asad-dev-vm/GroupIDSecurityService/1/Automate-ASAD-DEV-VM	
Identity Provider Image:					
Browse No Image Selected					

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.**

Q1	AD FS				
💱 File Action View Window Help		_ 8 ×			
	ervice	Actions			
Genvice Eqt Federation Service Propertie Eqt Federation Service Propertie C Revolte All Provies Trutt View C New Window from Here R A after h A arth Help Per Relying Party Trust	Cverview In several service components that are necessary to set up and manage a Federation Service. These include endports, cetificates, and published clasms. e	Service Edit Federation Service Properties Revoke All Proxies View New Window from Here Refresh Help			

Figure 26: AD FS Console – Service node

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

General	Organization Events
Feder	ation Service display name:
ADFS	for GID8
Examp	ole: Fabrikam Federation Service
Feder	ation Service name:
ADFS	.GID-8.Loc
Examp) ole: fs.fabrikam.com
	ation Service identifier
_	ADFS.GID-8.Loc/adfs/services/trust
	ole: http://fs.fabrikam.com/adfs/services/trust
	OK Cancel Apoly

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.

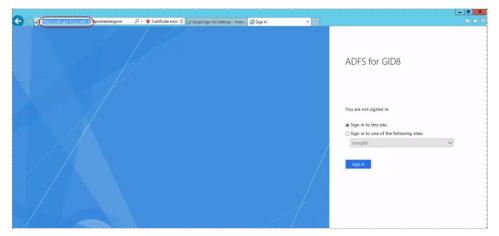


Figure 28: AD FS Authentication page

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:

🏟 File Action View Window Hel 🗢 🔿 🙍 📰 📓 📰	P						_ 6
AD FS	Certificates						Actions
Service Endpoints Certificates Cartificates Cartifica	Subject Service communications CHAPDPS SID & Lac Token-decrypting CHAPDPS Encryption - AD Token-signing CHAPDPS Suprem, ADPS	Issuer CN=ADFS.GID-8.Loc CN=ADFS Encryption - A CN=ADFS Signing - ADFS	Effective Date 11/6/2016 11/6/2016 11/6/2016	Expiration Date 11/5/2017 11/6/2017 11/6/2017	Status	Primary Primary Primary	Certificates Add Token-Signing Certificate Add Token-Decrypting Certificate Set Service Communications Certificate View New Window from Here Refeh Refeh Refeh Refeh Refeh
							CN=ADFS Signing - ADFS.GID-8.Loc View Cetrificate Set as Primary PHep

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.

General	Details	Certification P	ath		
88	Certi	ficate Inform	ation		
inst		t certificate i ertificate in t store.			
	Issued	to: ADFS Sign	ning - ADFS.GII	D-8.Loc	
	Issued	by: ADFS Sign	ing - ADFS.GII	D-8.Loc	
	Valid fr	om 11/6/2016	to 11/6/20	17	
		[Install Certifica	ste Is	suer Statemer
		l	Install Cel Unica	15	sue statene

Figure 30: Certificate Properties dialog box

3. Click the **Details** tab.

Chapter 1 - SAML Configuration for GroupID using AD FS

1		Cer	tificate	
General	Details	Certification Path		
Show:	<all></all>		~	
Field			Value	^
Ser Sig Sig	suer		V3 77 95 23 72 6b 6c 0e b3 4a 2b sha256RSA sha256 ADFS Signing - ADFS.GID-8.Loc	III
	lid from lid to		Sunday, November 6, 2016 10 Monday, November 6, 2017 1	Π
(white	bject		ADFS Signing - ADFS.GID-8.Loc	~
		E	dit Properties Copy to File	
		6,1	L Copy to rach	•

Figure 31: Details tab

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

Welcome to the Cort	ificate Export Wizard	
welcome to the cen	incate Export wizard	
This wizard helps you copy certil lists from a certificate store to y	icates, certificate trust lists and certificate revoc our disk.	ation
and contains information used to	a certification authority, is a confirmation of your protect data or to establish secure network s the system area where certificates are kept.	identit
To continue, click Next.		

Figure 32: Certificate Export Wizard – Welcome page

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

Export Fil Certi	e Format ficates can be exported in a variety of file formats.
Selec	t the format you want to use:
C	DER encoded binary X.509 (.CER)
0	Base-64 encoded X.509 (.CER)
C) Crywsographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	Include all certificates in the certification path if possible
0	Personal Information Exchange - PKCS #12 (.PFX)
	Include all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
0	Microsoft Serialized Certificate Store (.SST)

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**.

£* (Certificate Export Wiza	ard	
File	e to Export Specify the name of the file	you want to export	
	File name:		Browse
			4
			Next Can

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**.

Export Keys No Include all certificates in the certification path No File Format Base64 Encoded X.509 (*.cer)	ou have specified the following settings: File Name	C: \Users \Administrator \Desktop \Cert I
Hie Format Base64 Encoded X, 509 (*, cer)		
< III	21 W	
< III	<	>

Figure 35: Completion page

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

	Cert Export - Notepad	_ _ ×
File Edit Format View Help		
BEGIN CERTIFICATE		
MIIC2DCCAcCgAwIBAgIQd5UjcmtsDrNKK7XNVCgemzANBgkqhkiG9w0BAQsFADAo		
ISYwJAYDVQQDEx1BREZTIFNpZ25pbmcgLSBBREZTLkdJRC04LkxvYzAeFw0xNjEx		
DcwNjIzMTNaFw0xNzExMDcwNjIzMTNaMCgxJjAkBgNVBAMTHUFER1MgU21nbmlu		
vAtIEFER1MuR01ELTguTG91MIIBI1ANBgkghkiG9w0BA0EFAAOCA08AMIIBCgKC		
OEA2ps+wngBOhVxkdaPDzvgRgHT+dZZR/R5/ybNLyVijLBanNnR11/FzPzrIQuN		
x2IizoA600DOc+dcmpcw+x1MkdRSbL3yHvgatHE4Z9Z62WVa0JnVCqGrtSnLg1s		
Zdf2oYPFcKP9Ug0D8K6M57b1MHYrsU5sLgoN8eSGr0p+uyivq1HH01ghvs6Y1X3		
+A6U9OSx2ApA7mKbm2ihfhn+wUoN/5UmJ/IhINiwHaaEVV1pfxfBJ6FIkOfcqVJ		
NnJKSahBlligrbd046LBz3c/p3E77gWi+i0++t0+nrR0cREg0IM0iMyw6J/gFBJ		
pKjxpk9aDtwnIywkbbX+hOIDOIDAOABMA0GCSqGSIb3D0EBCwUAA4IBA0BHNzkh		
2ExYd+0fDIgQn8yeYKv1uYsu0zIMfb5CdFtMWumvjbdIZ1hRjkUQ3BiWpgB4Q0j		
AwaD7eAy/7dNMiW42v2R9r3UOcnh2vTa3Z+mv11wyhVXcAxGB1hXOHxGV/OMUTt		
Rx1UcNRFgWYxzrN70GLzXSr++4ahKiYKsV0700YVK0J1dvnnc6byUj6U335xEje		
tObJRURnjIue0uSk518y7T0I1B81ySgGa3oCHOnZ2Vst4a2xdVskO6Wdrm8Pu0y		
FUh99hAH1f/8iZYc5ra1x3wDh0AH/ti7cA3IJ1sLXUkj9XK9a/dsV6WMVTf1Kzv		
it+22z1f5fTaNetc		
END CERTIFICATE		

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).

sponse Signing:	Response Signing Method:	Request Binding:	
Enabled 🗸	RSA-SHA-256 🗸	Redirect 🗸	
sable GroupID Authentication:	Display On Login Page:	Logout Redirect:	
No 🗸	Yes 🗸		
entity Location:	Assertion Encryption:		
Identity is in Name Identifier of Subjer	Disabled 🗸		

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.

Monitoring	Identifiers	Encrypti	on S	ignature	. 1	Accepted (Claims
Organization	Endpoints	Prox	y Endpoi	nts	Notes	Adva	inced
pecify the en	dpoints to use f	or SAML	and WS	6-Federa	tionP	assive prot	ocols
URL			Index	Bindir	ng	Default	Re
SAML Ass	sertion Consur	mer End	lpoints				
https://g	jid8:4443/Group	DDSe	0	POST	Г	No	
		202		-			
		6					
		R					
		6					
		R					
		<i>⊊</i>					
		₽					
			2				
<			3				>
< Add SAML.			3/				>

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.

Response Signing:	Response Signing Method:		Request Binding:	
Enabled 🗸	RSA-SHA-256	~	Post	\sim
Disable GroupID Authentication:	Display On Login Page:		Logout Redirect:	
No 🗸	Yes	~		
Identity Location:	Assertion Encryption:			
Identity is an attribute element 🛛 🗸	Disabled	~		
Identity Location Attribute:				

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.

🗢 🔿 🙍 📰 🖬					
AD FS	Claim Descriptions				Actions
Service Endpoints	Name	Short Name	Claim Type	Publ ^	Claim Descriptions
Certificates	E-Mail Address Given Name	email given name	http://schemas.xmlsoap.org/ws/2005/05/identit http://schemas.xmlsoap.org/ws/2005/05/identit	Yes Yes	Add Claim Description.
Claim Descriptions	Name	unique_name	http://schemas.xmlsoap.org/ws/2005/05/identit	Yes	View
a 🚞 Trust Relationships	UPN	upn	http://schemas.xmlsoap.org/ws/2005/05/identit	Yes	New Window from Her
Claims Provider Trusts	Common Name	commonname	http://schemas.xmlsoap.org/claints@CommonName	Yes	
Relying Party Trusts	AD FS 1 x E-Mail Address	adfs1email	http://schemas.xmlsoap.org/claims/EmailAddress	Yes	Refresh
Attribute Stores	Group	group	http://schemas.xmlsoap.org/claims/Group	Yes	Help
a 🚞 Authentication Policies	AD FS 1 x UPN	adfs lupn	http://schemas.xmlsoap.org/claims/UPN	Yes	
Per Relying Party Trust	Role	role	http://schemas.microsoft.com/ws/2008/06/iden	Yes	UPN
	Sumame	family_name	http://schemas.xmlsoap.org/ws/2005/05/identit	Yes	Properties
	PPID	ppid	http://schemas.xmlsoap.org/ws/2005/05/identit	Yes	
	Name ID	sub	http://schemas.xmlsoap.org/ws/2005/05/identit	Yes _	🔀 Delete
	Authentication time stamp	auth_time	http://schemas.microsoft.com/ws/2008/06/iden	Yes ≡	R Help
	Authentication method	authmethod	http://schemas.microsoft.com/ws/2008/06/iden	Yes	-
	Deny only group SID	denyonlysid	http://schemas.xmlsoap.org/ws/2005/05/identit	Yes	
	Deny only primary SID	denyonlyprimarysid	http://schemas.microsoft.com/ws/2008/06/iden	Yes	
	Deny only primary group SID	denyonlyprimarygroupsid	http://schemas.microsoft.com/ws/2008/06/iden	Yes	

Figure 41: AD FS Console – Claim Descriptions

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

	UPN Properties
General	
Display name	5.
UPN	
Claim type:	
http://schem	nas.xmlsoap.org/ws/2005/05/identity/claims/upn
Description:	
The user prin	cipal name (UPN) of the user
The user prin	icipal name (UPN) of the user
The user prin	icipal name (UPN) of the user
Publish the that this F	is claim description in federation metadata as a claim type ederation Service can accept
Publish the that this F	is claim description in federation metadata as a claim type ederation Service can accept
Publish the that this F	
Publish the that this F	is claim description in federation metadata as a claim type ederation Service can accept
Publish the that this F	is claim description in federation metadata as a claim type ederation Service can accept
Publish the that this F	is claim description in federation metadata as a claim type ederation Service can accept

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).
- 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

(
	Username
	Supported Username Formats: [username] [name@domain] [domain\username]
	Password
	Identity Store: Adatum
	Sign In \rightarrow
	OR
	Wizard ADFS Authenti

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 <u>IDP login URL</u>.



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

sign-on.

- 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
- 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.
- Go to Azure Active Directory > Enterprise Applications and add a new application.

Microsoft Azure		P Search reso	urces, services, and docs			>_	8	0 ©	? @) qasim@nextsoluti Nor sou	
	Home > Next Solutions > Enterprise appl										
+ Create a resource	Enterprise applications - All ap Next Sources - Acute Acute Directory	plications									
All services	K Overview	+ New application									
Deshboard	Manage	Application Type Enterprise Applications	Applications status Any v	Application visibility Any	~	Apply	Reset				
All resources	All applications Application provy										
 App Services Function Apps 	Approaren prory User settings Security	NAME	HOMEPAGE URL	:		OBJECTIO				PPLICATION ID	
SQL databases Azure Cosmos DB Virtual machines	Conditional Access										
Virtual machines Load balancers Storage accounts	Sign-ins Audit logs Troubleshooting - Support										
Acure Active Directory	Troubleshoot New support request										
Advisor Security Center O Cost Management + Billing											
Help + support											

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**.

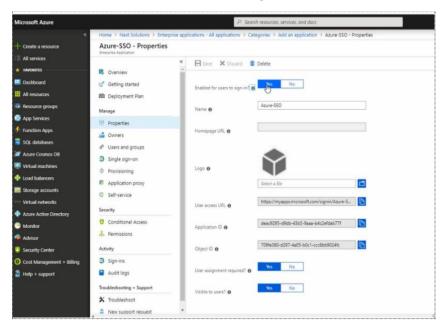
Microsoft Azure			,₽ Search resource	es, services, and docs			> 6 p @ 7
« + Create a resource	Home > Next Solutions > Enterpris	e applications	- All applications > Categories > Add an application	Add an application > Add yo		×	Add your own application 🛛 🗵
I All services	All (3034)		Add your own app				* Name 🛛
Dashboard	Business management (333)		Application you're	On-premises application	Non-gallery application	1	Azure-SSO 🗸
 All resources Resource groups 	Collaboration (419) Construction (8)	- 1	developing Register an app you're	Configure Azure AD Application Proxy to	Integrate any other application that you don't	I.	Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration
App Services Function Apps	Consumer (40)		working on to integrate it with Azure AD	enable secure remote access	find in the gallery	I.	steps to get the application working.
SQL databases	Content management (138) CRM (145)	- 1	Add from the gallery			1	Supports: SAML-based single sign-on Learn more
Azure Cosmos DB	Data services (143) Developer services (99)		Enter a name			I.	Automatic User Provisioning with SCIM
Load balancers Storage accounts	E-commerce (75)	-	Featured applications			n	Learn more Password-based single sign-on
· Virtual networks	Education (131) ERP (70)	_	box				Learn more
 Azure Active Directory Monitor 	Finance (248)	- 1					
🔷 Advisor	Health (61)		Box Con	cur Cornerstone Or	λ		
O Cost Management + Billing	Human resources (264) IT infrastructure (181)		DS	🔸 σ	e.		
Help + support	Mail (33)			▼ 0			
	Marketing (208)		Docusign Drop	obox for Busi G Suite			Add

Figure 47: Add an Application page

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

Microsoft Azure		.P Search resources, services, and docs	
Create a resource	Home > Next Solutions > Enterpr Azure-SSO - Overview	rise applications - All applications -> Categories -> Add an application -> Azure-SSO - Overview	Adding application 12:00 PM
All services	Enterprise Application		Application Azure-SSO added successfully
		« 🗓 Delete	
* FAVORITES	Sverview	Total Users	
Dashboard	getting started		
All resources	Deployment Plan	0	
😂 Resource groups	Manage		
🔇 App Services	11 Properties		
Function Apps	Properties Owners		
🧧 SQL databases		App usage between 10/10/2018 and 11/9/2018	
🥭 Azure Cosmos DB	x ^R Users and groups	App usage between 10/10/2018 and 11/9/2018	
Virtual machines	Single sign-on	ALMOSSV	
Load balancers	Provisioning		
Storage accounts	Application proxy		
	Self-service		
Virtual networks	Security	4	
Azure Active Directory	Condition@%Access		
Monitor			
🔷 Advisor	A Permissions	0	
Security Center	Activity	Oct 14 Oct 21 Oct 28 Nov 4	
Ocst Management + Billing	Sign-ins	O sign-ins	
Help + support	Audit logs		

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.

Microsoft Azure		P Search resources, services	s, and docr	>_ 🖓 🗘 🔍 🤉 🖓 🖓 🖓
+ Create a resource	Home > Next Solutions > Enterprise a Azure-SSO - Owners Enterprise Application	pplications - All applications -> Categories -> Add an a	application > Azure-SSO - Owners	Select Owners ×
All services All services All resources All resources All resources All resources All resources All resources	Correlew C ² Getting started BD Deployment Plan Manage	Add Ferrore Derust Connex Derust Name No application events found	S INCLASSING	Jefet seeker ur indr zu odend set. •
Function Apps SQL databases SQL databases Acure Cosmos DB Virtual machines Load balances Storage accounts	III Propenies Convers Convers Convers Convers Converse Converse Converse Converse Converse Converse Converse Converse Converse Converse Converse Converse Converse Converse Converse Converse Converse Converse C			Saland care
 Vehal networks Acure Active Directory Monitor Achicor Security Center Cost Management + Billing 	Security Conditional Access Conditional Access Actuaty Sign-ins			General general-descative Agence
2 Help + support	Audit logs Troubleshooting + Support Troubleshoot Nore: support New support result			Sea.

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**.

Microsoft Azure			\mathcal{P} Search resources, services, and docs	
« + Create a resource	Home > Next Solutions > Enter Add Assignment Next Solutions	rprise applications $ imes$	All applications > Categories > Add an application > Users and groups	Azure-SSO - Users and groups > Add
All services FAVORITES Dashboard	Users and groups None Selected	>	Select member or invite an external user o	Ŷ
Lasnboard All resources Resource groups	Select Role User	>	Qapim Ali qasim@nextsolutions.online	
App Services			QA qasim-test 5db533015b@nextsolutions.online	
SQL databases				
Virtual machines				
Storage accounts			Selected members:	Remove
 Azure Active Directory Monitor 			qasim@nextsolutions.online	
 Advisor Security Center 				
Ocost Management + Billing				
	Assign		Select	

Figure 51: Users and Groups page

SAML SSO configurations for the application

 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.

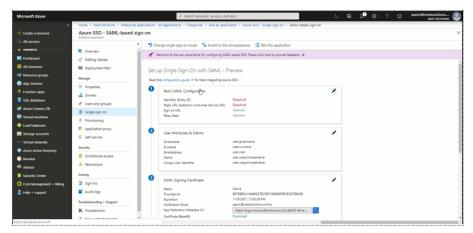


Figure 53: SAML-based sign-on settings page

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

Sale		
	re provided by Azure-SSO. You may either enter those values manually, or upload a pre-configured ed by Azure-SSO. Upload metadata file.	
Identifier (Entity ID) \tag	https://gid9/Group/DSecurityService/2/Azure	~
Reply URL (Assertion onsumer Service URL) 🜒	https://gid9/Group/DSecurityService/Samt?clientids.d7f30c95-8bc8-4d44-8902-6451d6ede5d5	~
 Set additional URL: 	5	
Sign on URL 🛛	Enter a sign on URL	

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*.

Sig	n in to continue to Azure
	Username
	Supported Username Formats: [username] [name@domain] [domain\username]
	Password
	Identity store: Azure
	Sign In →
	OR
	Azure-SSO

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.

Microsoft		
Sign in		
Email, phone, or Sky	/pe	
Can't access your accou	unt?	
	Back	Next
	Back	Next
	Back	Next

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 <u>Assign Users to log into GroupID using Azure AD</u> <u>SSO</u>.

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

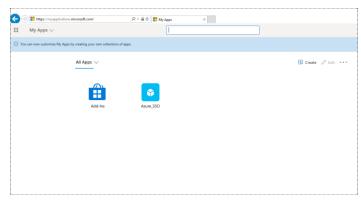


Figure 57: My App Portal

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.

() () () https://imanami-enline.okta.com			C Q, Search	☆ 台 ♣ ★ ♥
	okta			
	Sign In			
	L (L mass	0		
	Remember me	0		
	Sign In			
	Need help signing in?			

Figure 58: Okta login page

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

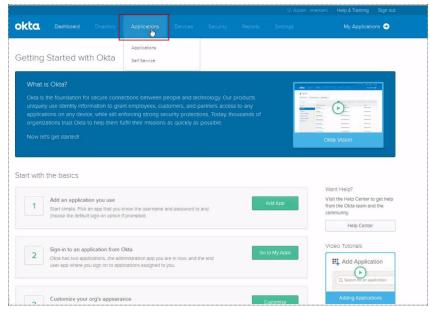


Figure 59: Okta Dashboard

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

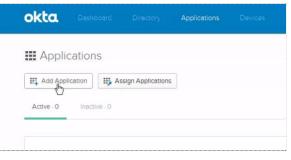


Figure 60: Applications page

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

okta Dashboard				My Applications 🔿
Add Application				← Back to Applications
Q			ALLABCDEFGHIJKLM	N O P Q R S T U V W X Y Z
Can't find an app Create New App		O TELADOC	Teladoc Okta Verified	Add
Apps you created (0)	-	&frankly	&frankly Okta Vertfied SAML	Add
INTEGRATION PROPERTIES			do-	
Any		10,000 ft	10000ft Okta Verified	Add
Supports SAML	_			
Supports Provisioning		ji)/domain	101domains.com Okta Verified	Add
CATEGORIES		123RF	123RF Okta Verfied	Add
All	5075			
Content Management	179	15Five	15five	Add
Collaboration	698	TOT IVE	Okta Venfied - SAML	Add
Consumer	190			
CRM	137	1&1	landt E-mail Okta Vertfied	Add
Data & Analysis	263			
E-Commerce	47			

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**.

. Create SAML In	egration					
1 General S	ettings		O Cor	figure SAML		
General Settings						
Арр пате		I				
App logo(optional)		Ø				
	Uple	bad Logo			Browse	a
App visibility			pplication icon to		е арр	

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.

okta 🜼	shboard	Directory	Applications	Devices	Security	Reports	Settings	My Applications 🕣
Create SA	AML Inte	egration						
G General Settings			2 Cor	nfigure SAML			3 Feedback	
A SAML Setting	gs							
GENERAL								What does this form do? This form generates the XML needed for the app's SAML request.
Single sign on U	irl		Use this for Reci	cipient URL and Destination URL				Where do I find the info this form needs?
Audience URI (S	P Entity ID) 🌘	>			N			The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should
Default RelaySt	ate 🕜	[f no value is set, a bi	ank RelayState	ls sent			outline what information you need to specify in this form.
Name ID format	0		Unspecified		*			Okta Certificate Import the Okta certificate to your identity Provider if required.
Application use	mame 👩		Okta username		*			➡ Download Okta Certificate
					Shov	v Advanced Settin	gs	
ATTRIBUTE ST	ATEMENTS (OPTIONAL)				LEARN MO	RE	

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.

	IENTS (OPTIONAL)		LEARN MORE
Name	Name format (optional)	Value	
	Unspecified +		¥ ×
Add Another			
			4
GROUP ATTRIBUTE	STATEMENTS (OPTIONAL) Name format (optional)	Filter	
	Unspecified *	Starts with +	×
Add Another			
Preview the SAM	L assertion generated from	the Information above	
	that will be used in the accertio	n - use it to verify the info you entered	above

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.

Create SAML Integ						
General Setting	ğs		O Co	nfigure SAML		3 Feedback
3 Help Okta Support unders	and how you co	nfigured this	application			
						Why are you asking me this? This form provides Okta Support with usefu
Are you a customer or partner?		an Okta custo a software ver		internal app integrate my app	with Okta	background information about your app. Thank you for your help—we appreciate it.
Is your app integration complete		, my app integr blication Netwo		for public use in	the Okta	

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:

okta Deshboard Directory Applications Devices Security Reports Settin	ngs My Applications 🔿
General Sign On Mobile Import. People Groups	← Back to Applications
Settings Edit	About SAML 2.0 streamlines the end user experience by not requiring the user to know
SIGN ON METHODS The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.	their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.
③ SAML 2.0	Application Username Choose a format to use as the default
Default Relay State	username value when assigning the application to users.
SAML 2.0 is not configured until you complete the setup instructions. View Setup Instructions	If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.
Identity Provider metadata is available if this application supports dynamic configuration.	

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).

	Opening metadata
ou have chosen to	open:
🏭 metadata	
which is: appli	cation/samImetadata+xml (2.3 KB)
from: https://i	manami-online.okta.com
What should Firefor	x do with this file?
0.0	Partura
O Open with	Browse
Save File	
Do this auto	matically for files like this from now on.
	inducing for thesince and item for our
	N OK Cance
	L2 UN Calica

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.

2		Library		
🔶 🔶 🍡 Organize 🔹 Clear	Downloads	.5	Search Downloads	,
 History Downloads 	metadat			e
Tags	2.3 KE	Remove From Hi Open Containing		
		<u>G</u> o To Download Copy Download		
		Clear Downloads		

Figure 69: Library dialog box

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

i I 🗋 🛄 🖛 I		Downloa	ds	
File Home St	nare View			
• الله 🗧 🕘 🕘	Computer 🕨 Local Disk (C:) 🕨 User	rs 🕨 administrator.GID-8 🕨 Downlo	ads	
🚖 Favorites	Name	Date modified	Туре	Size
E Desktop	📄 metadata	12/1/2016 12:54 AM	File	3 KB
🔰 Downloads 🔄 Recent places	La			
🥽 Libraries				
Documents				
J Music				
Pictures Videos				
Computer				

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.

 To create users manually or to import them into Okta, visit <u>https://help.okta.com/en/prod/Content/Topics/Directory/Directory_People.ht</u> <u>m</u>.

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

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.

Assign GroupID Okta Sign-On to People	×
Alex Ortiz Alex.Ortiz@Gid-8.loc	Assign
Umer Aslam umer.aslam@imanami.com	Assign
Ben.Sims@Gid-8.loc	Assign
Leo.Ferguson@GId-8.loc	Assign
	Done

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.

Assign GroupID Okta Sign-Or	n to People	×
User Name	Leo.Ferguson <mark>@Gid-6 loc</mark>	
	Save and Go Back Cancel	

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.

okta Dashboard	d Directory	Applications	Devices	Security	Reports	Settings	My Applications →
	GroupID Okt		3 people are assig	gned to the app			← Back to Application
General Sign On	Mobile Imp	ort People	Groups				
Applag to Recold							O Search
Assign to People Person & Username			Status				Q Search
				ng activation			Q Search_
Person & Username Alex Ortiz			Pendi				

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.

kta Dashbi	bard Directory	Applications Devic	es Security Reports Sett	ings My Applications 🔿
People		People are	being activated!	People Help
Add Person	Reset Passwords M	ore Actions *		
Q Search			AIIABCDEFGHIJK	LMNOPQRSTUVWXYZ
ILTERS	Person & User	mame	Primary Email	Status
everyone	4 Umer Aslam umer.aslam@ii	manami.com	umer.aslam@imanami.com	Active
Activated	3 Leo Ferguson		Leo.Ferguson@Gld-8.loc	Pending activation
Pending Activation	1 Leo Fergusoni	@Gid-8.loc		Activate
Password Reset	Alex.Ortiz@Gi	d-8.loc	Alex.Ortiz@Gid-8.loc	Passw Activate their Okta account
Password Expired	0 Ben Sims		Ben.Sims@Gid-8.loc	Password reset
Deactivated	0 Ben.Sims@Gid	5-8.loc		
	0			
Suspended				

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.

Advanced					
Response Signing:		Response Signing Method:		Request Binding:	
Enabled	~	RSA-SHA-256	~	Redirect	~
Disable GroupID Authentication:		Display On Login Page:		Logout Redirect:	
No	~	Yes	~		
Identity Location:		Assertion Encryption:			
Identity is in Name Identifier of Subject element	~	Disabled	~		

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*.

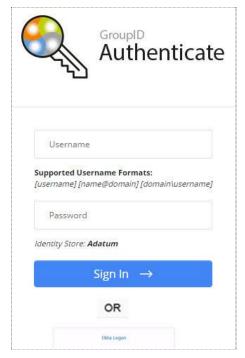


Figure 79: Login page with Okta button

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.

okta	
Sign In	
L Username	0
Password	0
Remember me	
Sign In	
Need help signing in?	

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.

okta		Q. Launch App	A Home	. ≜±	+ Add App	Admin
Work	+					
SelfService	PasswordCenter	Salesforce Customer Portal				

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.

- 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.



 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.
 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 $\stackrel{\checkmark}{=}$ to download the metadata file on your machine.

Configure GroupID in PingOne

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

ng									Welcome,	sabahat ali	Sign Of
hy S	Dashboard	Applications	Users	Setup	Account				? Help		
м	ly Dashboard Rep	ports									
You	ur PingOne dock	URL https://des	ktop.pingd	one.com/co	1-1689053281	.imanami					
No	otifications										
ſ	Update Your Co	prporate Logo									
	The corporate logo	is displayed on your	dock.								
1	Add Users										
	You have added 3 u	isers.									
Su	immary										
	-										
	Time Range: Toda	ay This Week La	st Week Th	is Month L	ast Month 1 Ye	ar 2 Years					
Logins											
24.	Oct 25. Oct	26. Oct 27. O	t 28. 0	ct 29. 0	ict 30. Oct	31. Oct	1. Nov	2. Nov	3. Nov		
	Axis Zoom: 5d 1	0d 1m 3m 1y	2y								
					(urrently Viewir	ng Oct 30, 2	2016 - Nov 8	5, 2016		
	5	:			6			Ω			

Figure 82: PingOne Identity Dashboard

2. Click the **Applications** tab.

ing							Welcome, <u>sabahat ali</u> Sig
ing	A Dashboard	Applications	Users	Setup	Account		? Help
М	ly Applications Ap	plication Catalog					
My	Applications	5				n /	Applications / My Applications
App	lications you've adde	d to your account are	listed here.	You can sear	ch by application name, of	description or entityId	
	Active applications an Details displays the a	re enabled for single s	ign-on (SSO).			
_	Details displays the e	application details.					
	Appli	cation Name	ту	ре	Status	Enabled	
	Fac	cebook	E	Basic SSO	Active	Yes	Remove
	Lin	kedin	E	Basic SSO	Active	Yes	Remove
	Offi	ice 365	E	Basic SSO	Active	Yes	Remove
	Sel	f service SAML	5	SAML	Active	Yes	Remove
	SSI	P	s	SAML	Active	Yes	Remove
A	dd Application -						Pause All SSO
	Search Application Ca	atalog					
	New SAML Applicatio						
1	New Basic SSO Appli	cation					
5	Request Ping Identity	add a new application	n to the appli	cation catalog	3		

Figure 83: Applications tab

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

Self service SAML	SAML	Active	Yes	Remove
SSP	SAML	Active	Yes	Remove
New Application	SAML	Incomplete	No	
1. Application Details				
Application Name	My Application			
Application Description	A short description of application.	fyour		
		Max 500 characters		
Category	Choose One	*		
Graphics	Application Icon For use on the dock		Application Logo For use on the pre- the dock	
	Max Size: 256px x 256	ipx	Max Size: 400px x	

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:

Application Name	Imanami GroupID App1	
Application Description	GroupID Self-Service Portal "Enterprise"	
	Max 500 cha	n aracters
Category	Information Technology	*
Graphics	Application Icon For use on the dock Network Change Mar: Stor: 256px x 256px	Application Logo For use on the previous version of the dock
NEXT: Application Configuration		Cancely Continue to Next Step
Add Application +		Pause All SSO

Figure 85: Application Details page (2)

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

I have the SAML configuration	I have the SSO I	URL
You will need to download this SAML metadat	a to configure the application:	
Signing Certificate	PingOne Account Origination Certificate	e •
SAML Metadata	Download	A
rovide SAML details about the application yo	u are connecting to:	
Protocol Version	SAML v 2.0	
Upload Metadata	Select File Or use URL	
Assertion Consumer Service (ACS)	https://sso.example.com/a/sso.saml2	•
Entity ID	example.com/a	
Application URL		
Single Logout Endpoint @	example.com/slo.endpoint	
Single Logout Response Endpoint @	example.com/sloresponse.endpoint	
Single Logout Binding Type	Redirect OPost	
Primary Verification Certificate @	Choose File No file chosen	
Secondary Verification Certificate @	Choose File No file chosen	

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.

My Applicatio X 🕒 Generate Url	+ imanami 🛛 🗙 🚺					
https://admin.pingone.com/w	eb-portal/cas/connectio					
	R d	1 BOUNDOR	UBBL OOO	num	(Chord)	- Commenter -
	in	Linkedin	Basic SSO	Active	Yes	Remove
	0	Office 365	Basic SSO	Active	Yes	Remove
		Self service SAML	SAML	Active	Yes	Remove
		SSP	SAML	Active	Yes	Remove
		New Application	SAML	Incomplete	No	
		the necessary application provi Application Attribute iden d new attribute	tity Bridge Attribute or Liter			quired
	NEXT: R	eview Setup		Cance	I Back Save &	Ext Save & Publish
	Add Applicati	on +				Pause All SSO Ø
	© 2003 - 2016 Ping ide	ntity Corporation. All rights reserv	6d.			Privacy Terms About

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.

Application Attribute	Identity Bridge Attribute or Lite	ral) blue	Required
Application Attribute	Identity bridge Attribute of Lite		Required
1 I	Name or Literal	As Literal Advanced	e ×
Add new attribute			
Add new attribute			

Figure 88: New row for adding authentication attribute

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

Advanced Attribute Options			
Advanced Attribute	Options for		
Advanced Attribute Options			
lameFormat @			
Attribute Mapping			
'ou can build an attribute mapping i	ising multiple source attributes, literals	and transformation functions.	
or example, SAML_SUBJECT can	be (where each attribute value is a sep	parate entry):	
<pre>subject = firstName + "." + la</pre>	tName + "@" + domainName		
IDP Attribute Name or Litera			
1 Name or Literal	As Literal	• @	

Figure 89: Advanced Attribute Options dialog box

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

NameFormat @	I	
	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified	
	urn:oasis:names:tc:SAML:2.0:attrname-format:uri	
	urn:oasis:names:tc:SAML:2.0:attrname-format.basic	

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.
- 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 dropdown is displayed. Select the **Email** option.

1	DP Attribute Name or Literal Value	As Literal Function	
1	E-Mail	As Literal	۰.
	Email		
	First Name		
	Last Name		

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.

	plications are enabled for single sign-o splays the application details.	n (SSO).			
	Application Name	Туре	Status	Enabled	
f	Facebook	Basic SSO	Active	Yes	Remove
	Imanami GroupID App1	SAML	Active	Yes	Remove
in	LinkedIn	Basic SSO	Active	Yes	Remove
0	Office 365	Basic SSO	Active	Yes	Remove
	Self service SAML	SAML	Active	Yes	Remove
	SSP	SAML	Active	Yes	Remove

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.

etadata File:		
Choose File No fihosen	Load File	

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

- 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.

Response Signing:	Response Signing Method:		Request Binding:	
Enabled 🗸	RSA-SHA-256	~	Post	
Disable GroupID Authentication:	Display On Login Page:		Logout Redirect:	
No 🗸	Yes	~		
Identity Location:	Assertion Encryption:			
Identity is in Name Identifier of Subjev	Disabled	~		

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:

		Welcome, <u>sabahat a</u>
Users Setup Account		? Help
/ Service		
	n / U	sers / Directory / Users
Search Advanced Search	All Users	T
 Username 	Status	Action
sabahat	Enabled	Edit -
bensims	Enabled	Edit
tanveer	Enabled	Edit -
		R
	Username sabahat bensims tanveer	y Service

Figure 95: Users page

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

User		ħ	Users / Directory / Users
			Cancel
	Password		
	*New Password	I	
	*Confirm New Password		
	Attributes		
	* Username		
	Name	Title	
		First Name	
		Middle Name	
		Last Name	
		Suffix	
		Formatted Name	

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

2	
User	name
	ed Username Formats: ne] [name@domain] [domain\username]
Pass	word
Identity :	Store: Adatum
	Sign In \rightarrow
	OR
	Ping One

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.

NOTE

 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.
 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.

onelogin	USERS APPS DEVICES ACTIVITY SETTINGS	✓ UPGRADE NOW	0 💧 Umer
	App Home Q III III NEW APP		
	Imanami		
	0		
	SAML Test Conne		
			VIDEAS



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*.

USERS APPS DEVICES ACT	IVITY SETTINGS	📌 UPGRADE I	iow 🧿 💧 Un
Find Applications		SUGGEST AN APP	
Q search I			
Accounting (267)	Entertainment (12)	Professional Services Automation (8)	
Advertising (28)	ERP (28)	Project Management (78)	
Airlines (24)	Events (18)	Public Relations (7)	
Analysts (10)	Expense Management (28)	Publishing (22)	
Analytics (97)	Fax (14)	Purchasing (1)	
Answer Management (1)	File sharing (68)	Quality Management (3)	
Appointment Scheduling (14)	Financial services (144)	Real estate (37)	
Automated Testing (2)	Fitness (1)	Recognition (4)	
Automotive (62)	Food Delivery (2)	Recruiting (70)	
Backup (36)	FTP (2)	Remote Support (11)	
Banking (66)	Graphics (26)	Reporting (5)	
Billing (28)	GRC (1)	Research (12)	V IDEA

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.

onelogin	JSERS APPS DEVICES ACTIVITY SETTINGS		VPGRADE NOW	Umer
	Find Applications	SUGGEST AN APP		
	Roogle SAML Quicklink Google Inc	SAML2.0		
1	Intralinks SAML OneLogin, Inc	SAML2.0		
	OneLogin, Inc.	SAML2.0		
	Pilot Catastrophe SAML (IdP) OneLogin, Inc.	SAML2.0		
	SAML Test Connector (IdP) Onst.ogin, Inc.	SAML2.0		
	SAML Test Connector (IdP w/ettr) OneLogin, Inc.	SAML2.0		
	SAML Test Connector (IdP w/attr. incl group transform) OrneLogin, Inc.	SAML2.0		
	SAML Test Connector (IdP w/ attr w/ sign response) Onst.ogin, Inc.	SAML2.0		
	SAML Test Connector (IdP) w/encrypt Onst.ogin, Inc.	SAML2.0		
	SAML Test Connector (IdP) w/ NameID (Unspec) Onst.ogin, Inc.	SAML2:0		
	SAML Test Connector (SP) OneLogin, Inc.	SAML2.0		PIDEAS

Figure 100: List of SAML applications

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

	Configuration		
Portal	Display Name GroupID <u>SAML</u> (JDP) for Users Portal Visible no protal Comparison Rectangular Icon Upload an icon with an aspect-ratio of 2.6.1 as either a transparent. PNG or .SVG	Square Icon Upload a square icon at least 512x512pc as either a transparent. PNG or .5VG	

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:

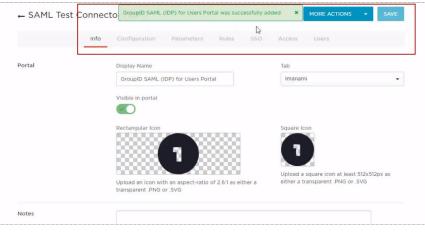


Figure 102: Create New App page (2)

Set Consumer URL and Audience URL

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

Audience Audience Recipient ACS (Consumer) URL Validator* ACS (Consumer) URL Validator Validates the ACS URL when initiated by an AuthnRequest ACS (Consumer) URL* Required Required	← SAML Test Connec	or (IdP) MORE ACTIONS - SAVE
Audience Audience Recipient ACS (Consumer) URL Validator* ACS (Consumer) URL Validator Validates the ACS URL when initiated by an AuthnRequest ACS (Consumer) URL* Required Required	Info	Configuration Parameters Rules SSO Access Users
Recipient ACS (Consumer) URL Validator* "Required. Regular expression - Validates the ACS URL when initiated by an AuthnRequest ACS (Consumer) URL* "Required	Application Details	RelayState
ACS (Consumer) URL Validator*		Audience
ACS (Consumer) URL Validator* Required. Regular expression - Validates the ACS URL when initiated by an AuthnRequest ACS (Consumer) URL* *Required	2	Recipient
Required. Regular expression - Validates the ACS URL when initiated by an AuthnRequest ACS (Consumer) URL		
ACS (Consumer) URL*		
Single Legent UDI		*Required
Single Logout ORL		Single Logout URL

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.

	ctor (IdP)					
Info	Configuration	Parameters	Rules	Access	Users	
credentials are						
Credentials are Configured by admin	Configured by adm	nins and shared by	all users			
		nins and shared by	all users			Add parameter

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

n on method ML2.0 09 Certificate tandard Strength C ange [View Details ML Signature Algor HA-256 ier URL ttps://app.onelogin	s rithm	8-bit)						
ior URL	•							
		tadata/6030	251	ß		Da		
D Endpoint (HTTP)	v.onelogin.com/1							
			/http-redire	ici 🖍				
en	Endpoint (HTTP ps://imanami-de Allow assumed u n enabled, admii ged by the acco	Endpoint (HTTP) ps://imanami-dev.onelogin.com/ Allow assumed users to sign intr n enabled, admins who assume	Endpoint (HTTP) ps://imanami-dev.onelogin.com/trust/sami2, Allow assumed users to sign into this app n enabled, admins who assume users can si eed by the account owner. Note that the ac	Endpoint (HTTP) ps://imanami-dev.onelogin.com/trust/sam/2/http-redire Allow assumed users to sign into this app nenabled, admins who assume users can sign into this ged by the account owner. Note that the account owner	ps://imanami-devonelogin.com/httst/samt2/http-redirect	Endpoint (HTTP) ps://imanami-devonelogin.com/trust/samt2/http-redirect Allow assumed users to sign into this app metabled, admins who assume users can sign into this app with their idd eque by the account owner. Note hat the account owner can also complex	Endpoint (HTTP) ps://imanami-devonelogin.com/trust/samt2/http-redirect Allow assumed users to sign into this app metabled, admins who assume users can sign into this app with their identity. This see get by the account owner. Note that the account owner can also completely diable to	Endpoint (HTTP) ps://imanami-devonelogin.com/trust/samt2/http-redirect C

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.

	Info	Configuration	Parameti	ers' Rules	Access	Users		
		All roles	•	All groups	•		UNMATCHE	D USERS
User								
Ben Sims								

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.

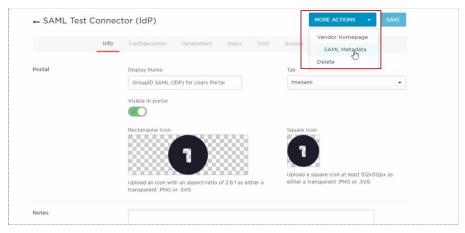


Figure 107: Download metadata file

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.)

		ided Metadata file	
Metadata File:	_		
	Browse	Load File	
	ß		

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

 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.

Advanced					
Response Signing:		Response Signing Method:		Request Binding:	
Enabled	~	RSA-SHA-256	~	Post	,
Disable GroupID Authenticatio	n:	Display On Login Page:		Logout Redirect:	
No	~	Yes	\sim		
Identity Location:		Assertion Encryption:			
Identity is in Name Identifi	er of Subject	Disabled	~		

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.

SAML Test Co	onnector (IdP)		MO	REACTIONS - SAVE
	Info Configuration	Parameters Rules S	SO Access U	sers
	All roles	All groups	•	UNMATCHED USERS
User				
Ben Sims				
Umer Aslam				

Figure 110: Users page

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

JSERS APPS DEVICES	ACTIVITY SETTINGS	
All Users		MORE ACTIONS - NEW USER
Q search users	Show Filters	
alex ortiz alex.ortiz@gid-8.loc		Last logged in about 1 hour ago
Ben Sims ben.sims@gid-8.loc	Default	Last logged in about 1 hour ago
Umer Aslam umer.aslam@imanami.com	Default account owner	Last logged in about 1 hour ago

Figure 111: All Users page

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

USERS APPS	DEVICES	ACTIVITY	SETTINGS			
← New User						CANCEL SAVE USE
				User Info		
		Active	2			
		First Nam			Last Name *	
		Email			Username	
		Phone Nu	mber		Manager Choose a manager	•
		Company			Department	
		Title				
Directory Details		Show Dire	ectory Details			
		SHOW DIFE	Detens			
Notes About This U	ser					

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.

← Leo Ferguson	Leo Ferguson was successfully	reated. X MORE ACTIONS -
	User Info Authentication Ap	pplications Activity
Authentication	Authenticated By	
	OneLogin	
	default is Default policy 👻	
Open ID	OpenID 😡	Change
	leo ferguson	
Multi-factors	Multi-factor authentication	
	No device registered.	
	Temporary OTP Token 🚱	Generate

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.

← Leo Ferguson		MORE ACTIONS + SAVE USE
	User Info Authentication Appli	ications Activity
Roles	Applications	
Default		

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:

Assign	New Login To Leo Ferguson
This login will override a Select Application	Iny apps assigned via roles. GroupID SAML (IDP) for Users Portal
	GroupID SAML (IDP) for Users Portal
	SAML Test Connector (IdP)

- 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:

	Leo Ferguson
Enabled	✓ Allow users to sign in
Email)eo.ferguson@gid-8.loc
	3

Figure 116: Edit app for User dialog box

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

Figure 115: Assign New Login dialog box

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

🗕 Leo Ferguson		MORE ACTIONS - SAVE USER
	User Info Authentication Applications	Activity
Roles	Applications	+
Default	GroupID SAML (IDP) leo.ferguson@gid-8.loc for Users Portal	Admin-configured

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**.

← Leo Ferguson			MORE ACTIONS
	User Info Authentication	Applications Activ	Assume User Change Password
	Active		Force Logout Send Invitation Show User Details
	First Name *	Last Name *	Reapply Mappings
	Leo	Ferguson	Delete
	Email	Username	Download PKI cert
	leo.ferguson@gid-8.loc	leo.ferguson	Create New User
	Phone Number	Manager	Create New Sub User

Figure 118: Change Password option

14. The following dialog box is displayed:

New Password	1	[₂
	Force user to upd	late
	Force user to change t time they log in.	their password the next

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*.

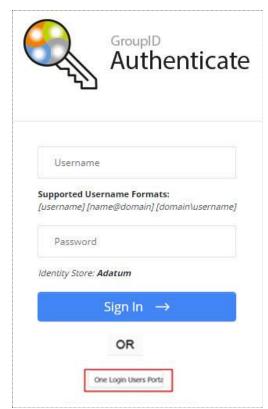


Figure 120: Login page with OneLogin button

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.

C	onelogin	
Email		
Password		
	LOG IN	
ORGOT PASSWO	RD	

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.

onelogin			Administration
	Q Search		
Frequents Company			Browse App Store
Coffice 365	Password Center	Self-Service	
Office 365	PasswordCenter	SelfService	

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 thirdparty 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.

((+)) SAML Providers	Applications	💮 Generat	e URL's 🔯 Authenticati	ion Settings			
Create Application							
Basic							
Name:			Consumer Url		Entity ID/Audience:		
Status:			Identity store:		Claims		
Enabled Identity Provider Image:		~	Cheoti	~			
Browse No Im	age Selected						
Advanced							~
Metadata							~
						Cancel	Create Application

Figure 123: Create Application page

- 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

Advanced						^
Response Signing:		Response Signing Method	Ŀ	Response Binding:		
Enabled	~	RSA-SHA-256	~	Post	~	
Assertion Encryption:		Single Logout URL:				
Disabled	~					

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** dropdown 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.

Metadata					~
Provider Issuer		Provider IDP Redirect Endpoint		Provider IDP POST Endpoint	
https://win-gidf/servers4443/groupidsecurityservice/sami/app/metadata/75cfl		https://win-gid9servers443/groupidsecurityservice/sami/sso/redirect/75cf9affiltervice/sami/sami/sso/redirect/75cf9affiltervice/sami/sami/sami/sami/sami/sami/sami/sami		https://win-gid9serverx4443/groupidsecurityservice/saml/sso/post/75cf9a9af5	
Provider Signing Certificate		Single logout Endpoint(POST)		Login URL	
BEGIN CERTIFICATE MIIDM#CCAbusAw/BalODRrumO162r7OICytril Zv/JANRskobkiG9w	Â	https://win-gid9servery6443/groupidsecurityservice/sami/sio/post/75cf9a9af7	Ū	https://win-gid9server/4443/groupidsecurityservice/saml/login?applicationid*	Ū
DBAQUFABBBINTSWFQYDVQQD HYNASQBNAGEAbgBING0AaQBIAEEAcgBvAHUAcABJAEQAXwBDAGU AcgB0AGAZgBpAGMAYQBDAGUw					
Neukor Ngung Centhone —BEGIN CERTIFICATE MIDMECK AnugAwithAgQORCumQ162/20[Cr.ttll.2y]ANBgkr/bi6/9w MQACUFABBBMENPC/VDQQO HIYASQBAACABgBAACANgBAACuk AgBAACAABgBAACANgBAACuk		Single legent Endpoint(POT) Inspanlining gifterversikkärgroupd securitysen sakamitskärgess 73cfahlsf7	Ũ	tage VM. https://www.goffers-erskittlgroupdisecurityservisitaen/Appillage/astoriet	ũ

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.

			uthentication Settings
Authentication Settings			
Base URL https://win.giddserver.44	143 Ioad PFX		Signing Centificate BEGIN CERTIFICATE MIIDMzCCAhugAwiBAgQDaRcumQ162rZOJCxtdLZy/JANBgkqhkiG9w0 BAQUFADBBMTswPQDVQQD HJYASQBtAGEAbgBhAG0AaQBfAEcAcgBvAHUAcABJAEQAXwBDAGUA cgB0AGkAZgBpAGMAYQB0AGUw

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.

Import Windows exported Certifica	te File(.pfx)	>
Select your file to import		
Browse	Password	Load Certificate File

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.
- 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.

🛺 Authorization Manager			- 🗆 X
🛐 File Action View Window	Help		- 8 ×
Authorization Manager GroupIDAuthStore.config GroupIDAuthApplication GroupIDAuthApplication Definitions Role Assignments GroupID Administri GroupID Helpdesk	Name Administrator(/EE\Administrator) Domain Admins(/EE\Domain Admins) Ben Sims(Ben.Sims@jee.local)	Type User Group User	Description
< >	<		>

Figure 128: AzMan Console

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