

intelliHR SSO Configuration

Windows Server ADFS Configuration

Requirements Instructions Create a relying party trust Edit the claims issuance policy Configure intelliHR Settings Configure intelliHR user for SSO

Azure AD Configuration Requirements Instructions Configure an App in Azure AD Configure intelliHR Settings





Windows Server ADFS Configuration

Requirements

The following requirements are required before continuing this guide.

- 1. An intelliHR account
- 2. A Microsoft Windows Server running Active Directory Federation Services (ADFS). This guide uses Windows Server 2019.

Instructions

Create a relying party trust

1. Open AD FS Management



2. Go to the Relying Trusts folder and click Add Relying Party Trust

AD FS		the set	3.104.55.122	_ 8 × _	-
File Action View Window Help					
• 🔿 🙍 📅 📓 📅					
AD FS	Relying Party Trusts				Actions
Service Arbibular Stores Arbibular Stores Arbibular Stores Centrolates Centrolates Centrolates Centrolates Centrolates Centrolates Centrolates Seope Descriptions Weit Application Prays Access Control Policies Reinge Bark / Insta- Centrol Policies Application Groups	Digday Name	Erabled Type kloreter	Access Cartrol Policy		Region 2 herb. Starts A 64 Relying 9 arty Trust Vear New Window from Here Image: Starts and Starts Image: Starts and Starts Image: Starts and Starts Image: Starts and Starts

3. Select Claims aware and click Next







4. Select Import data about the relying party... and use the URL https://<your name>.intellihr.net/saml2/metadata then click Next

翰 Add Relying Party Trust Wi	zard X
Select Data Source	
Steps • Welcome • Select Data Source • Choose Access Control Policy • Ready to Add Trust • Finish	Select an option that this wizard will use to obtain data about this relying party: (e) Import data about the relying party published online or on a local network. Use this option to import the necessary data and certificates from a relying party organization that publishes ts federation metadata address (host name or URL): Inttps://sso-demo.intellindev.net/sami2/metadata[Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported if seferation metadata to afile. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata to afile location: Federation metadata by manually Use this option to manually input the necessary data about this relying party organization.
	< Previous Next > Cancel

5. Select a display name to use for the trust and click Next

翰 Add Relying Party Trust Wizard					
Specify Display Name					
Steps	Enter the display name and any optional notes for this relying par				
Welcome	Display name:				
Select Data Source	so-demo.intellihrdev.net				
 Specify Display Name 	Notes:				
 Choose Access Control Policy 					
Ready to Add Trust					
 Finish 					

6. Optionally, configure access restrictions on who can use SSO

輸 Add Relying Party Trust	Wizard		×
Choose Access Contr	ol Policy		
Steps	Choose an access control policy:		
Welcome	Name	Description	^
Select Data Source	Permit evenuose	Grant access to evenyone	
Specify Display Name	Permit everyone and require MFA	Grant access to everyone and requir	
 Configure Certificate 	Permit everyone and require MFA for specific group	Grant access to everyone and requir	
Configure Contribute	Permit everyone and require MFA from extranet access	Grant access to the intranet users an	
Configure ORL	Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and requir	
Configure Identifiers	Permit everyone and require MFA, allow automatic device registr	Grant access to everyone and requir	
 Choose Access Control Policy 	Permit everyone for intranet access	Grant access to the intranet users.	v
Ready to Add Trust	C	,	
Datala	Policy		
	Pemit everyone	user will be permitted access for this	
	application.		
	< Pres	vious Next > Cancel	

7. Select default options for the remainder of the wizard.





Edit the claims issuance policy

1. Edit the claims issuance policy



2. Click Add Rule

The foll	wing transform rul	rs specify the clai	ns that will be sent to t	he relying party.
Order	Pule Name		Issued Cal	TR
	_			1
		la Daman	0.4	

3. Select Transform an incoming claim and click Next



4. Create a transformation for the property type of your choice to **Name ID in Email format**. In this case we are using UPN. Then click **Finish**.

Edit Rule - UPN to Name	ID	×				
You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.						
Claim rule name:						
UPN to Name ID						
Rule template: Transform a	n Incoming Claim					
Incoming claim type:	UPN	\sim				
Incoming name ID format:	Unspecified	\sim				
Outgoing claim type:	Name ID	\sim				
Outgoing name ID format:	Outgoing name ID format:					
Pass through all claim v Replace an incoming d	Pass through all claim values					
Incoming claim value:	an rade win a another outgoing claim value	_				
Outgoing claim value:	Browse					
O Replace incoming e-ma	il suffix claims with a new e-mail suffix					
New e-mail suffix:						
	Example: fabrikam.com					
View Rule Language	OK Cancel					





5. Verify that the rule has been added and click OK



Configure intelliHR Settings

- 1. Logon to intelliHR
- 2. Navigate to Settings->SSO

	Compliance	~	Access and Permissions	
đa	Org Chart		Permissions Assign and edit permission groups	
188	People		Cinale Circ. en	
٢	Automation	~	Access SSO (Single Sign-On) settings	
۲	Settings	_		

3. Click Create SSO idP

SSO IdPs	
	No SSD IdPs configured

Configure the required options, taking note of the URLs used and click Create SSO idP. Note: you can obtain the x509 Certificate at the following URL https://<your ADFS server>/FederationMetadata/2007-06/FederationMetadata.xml. Use the signing certificate from the xml.

Create SSO IdP	
Name - required	
Demo SSO	
Enabled	
Entity ID - required	-
https://ec2-54-79-24-127.ap-southeast-2.compute.amazonaws.com/adfs/services/trust	
Single Sign-On URL - required	
https://ec2-54-79-24-127.ap-southeast-2.compute.amazonaws.com/adfs/ls	
SLO Endpoint URL - required	
https://ec2-54-79-24-127.ap-southeast-2.compute.amazonaws.com/adfs/is	
Name ID Format - required	
Email address	× *
x509 Certificate - required	
This can either be the full certificate or the fingerprint	
AuthnContextClassRef	
	~
Multiple choices are allowed	
Authn Comparison - required	
Exact	Ŧ
Create SSO IdP	





Configure intelliHR user for SSO

1. Go to Settings->User Accounts

Settings		
	Clear	
Access and Permissions		
Permissions Assign and edit permission groups		User Accounts

2. Click Edit on the user to enable for SSO

sarah (S <mark>ara Hudson</mark>)			
SSO ID: Not set			
MFA Enabled: ×Not Enabled Group Memberships • System Administrator			
69 VIEW	🖋 EDIT	A MANAGE GROUPS AND PERMISSIONS	💼 DELETE

3. Set the SSO ID of the user and save. The SSO ID should be the user's UPN or other unique identifier setup in the idP.

	SSO ID
callum.pember@sso-demo.local	
ID passed from your IdP to match against this user.	

4. The user can now login via SSO







Azure AD Configuration

Requirements

- 1. An intelliHR account
- 2. An Azure AD tenancy

Instructions

Configure an App in Azure AD

1. Logon to the Azure AD portal at https://portal.azure.com and click Enterprise Applications



2. Click New Application



3. Click Non-gallery Application







4. Give the application a name and click Add

Add your own a	pplication	
Name * (i) intelliHR SSO	~	7
Once you decide on a simple configuration s	name for your new application, click the "Add" button below and we'll walk you through some teps to get the application working.	-
Supports: 🕕		
SAML-based single si Learn more	gn-on	
Automatic User Provis	sioning with SCIM	
Password-based singl Learn more	e sign-on	

5. Click on Users and Groups

	intelliHR SSO Overview	
	«	
👢 Ov	verview	Properties
De	eployment Plan	Namo (i)
🗙 Dia	agnose and solve problems	intelliHR SSO
Manage		Application ID
II Pro	operties	1274cf78-b3f
🚨 Ov	vners	Object ID 🕕
路 Us	ers and groups	668f84e8-018
∋ Sir	ngle sign-on	Getting Started
Pro	ovisioning	
🐯 Ap	plication proxy	👤 1. Assign
😔 Se	If-service	Provide sp

6. Click Add User



- 7. Add users as required
- 8. Select **Single sign-on** from the menu







9. Select SAML

10. Save the following details for quick reference to configure the intelliHR side



11. Click on Edit

t up Single Sigr	-On with SAML		
d the configuration g	ide 🖉 for help integrating int	telliHR SSO.	
Basic SAML Co	nfiguration		Ø
Identifier (Entity	(ID)	Required	
Reply URL (Asse	rtion Consumer Service URL)	Required	
Sign on URL		Optional	
Relay State		Optional	
		Optional	

12. Use the URLs supplied in the image below, replacing **sso-demo.intellihrdev.net with <your name>.intellihr.net** and save the configuration.

Basic SAML Configuration			
🚽 Save			
Identifier (Entity ID) * 🕕			
The default identifier will be the audience of the SAML response for IDP-initiated SSO			
	Def	ault	
https://sso-demo.intellihrdev.net/saml2/metadata	<u>~</u>	()	Û
Reply URL (Assertion Consumer Service URL) * 💿			
The default reply URL will be the destination in the SAML response for IDP-initiated SSO			
	Def	ault	
https://sso-demo.intellihrdev.net/saml2/acs		(1)	Û
Sign on URL ①			
https://sso-demo.intellihrdev.net/auth/login			~
and have a second se			
Relay State 🕕			
Enter a relay state			
Enter a renzy surve			
logout Ur			
			~ 1

13. Click on the edit button in section 2 to edit User Attributes and Claims

2	User Attributes & Claims		
	givenname	user.givenname	
	surname	user.surname	
	emailaddress	user.mail	
	name	user.userprincipalname	
	Unique User Identifier	user.userprincipalname	

14. Edit Name ID to be the value you wish to use for SSO (in this case email address) and save.

Value	
user.mail [nameid-format:emailAd ***	





Configure intelliHR Settings

- 1. Logon to intelliHR
- 2. Navigate to Settings->SSO



3. Click Create SSO idP

terrings / statutes	
SSO IdPs + Create SSO MP	
	No SSO IdPs configured

4. Configure options as shown in the image below. For x509 certificate, this can be found when visiting the Identity Provider metadata URL, which will provide an XML document that looks like the below:

<roledescriptor xs<br=""><<u>KeyDescriptor u</u> -<x509data> -<x509data> GWjdbUFR UAB5TyPU 241xmWim</x509data></x509data></roledescriptor>	Istype = "fed:SecurityTokenServiceType" protocolSupportEnumeration = "h se = "signing">	ttp://docs.oasis-open.org/wsfed/fed MAYDVOQDEyINaWNyb3NvZnOgg VytoHFO/19Yf0EDNCCQoKUGPs/ TISFingScknOK BPC/NIZOBEFEDTaFavVwcDed6E	eration/200706"> 2Xp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0a uucLKfY/Q0q5MbD9CAlYIn4PJnZJxhZ+lDcT pxf4401HLDVMC4/g54b274aFr421Prf6YYh	WZpY2F0ZTAel tvil94
pchVSsfpej	inTorSjsFOSinThlini OwrpeinToswitaJnioski 41(1)wyteolpysj + Inicolayi inTprBm8G+kCWunqQ0px8DkIj++7ZMdfI2IraxkklCvubTHHOAI9AaJX0Lmi oHuCPO5haMmakt1rkH720Nbc+oFByEEnVoorXOdI2xHaXNobiFCOw9HOU	W1Ab0Ceg4LqgWIn8fg1O/l6ndrSj:	CopXYRVV6x	
<th>ficate></th> <th>62(D\$50+5)</th> <th></th> <th></th>	ficate>	62(D\$50+5)		
/				
	Create SSO IdP	0000000		
	Azure SSO Demo			
	Enabled			
	Entity ID - required	00000000		
	https://sts.windows.net/8edc0761-49d9-43aa-9dfc-13f00761405b/			
	Single Sign-On LIDL - required	Set up intelliHR SSO		
	https://login.microsoftonline.com/8edc0761-49d9-43aa-9dfc-13f00761405b/saml2	You'll need to configure the app	lication to link with Azure AD.	
	unbailieBuurussestaumesesti essestet vess vess sets tetsestet vessianus	Login URL Azure AD Mentifier	https://login.microsoftonline.com/8edc0761- https://stawindows.pat/8edc0761-49d9-43au	
	SLO Endpoint URL - required	Logout URL	https://login.microsoftonline.com/common/s	
	https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0	View step-by-step instructions		
	Name ID Format - required		0000000000000000	
	Email address	× - 00000000		
	x509 Certificate - required			
	This can either be the full certificate or the fingerprint			
	AuthnContextClassRef			
	No AuthnContext	 300000000 		
	Multiple choices are allowed			
	Authn Comparison - required			
	Exact	 900000000 		
	00000 550 1/0			
	Create 330 run			

5. The user can now login via SSO



