

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		line 🕶	3.104.55.122	_ @ ×	-
File Action View Window Help					
• 🔿 🙍 📅 📓 📅					
AD FS	Relying Party Trusts				Actions
Service Anthold Scress Anthold Scress Anthold Scress Centricates	Digday Name	Enabled Type kinneler	Access Cared Palcy		Belging Party Trust. Add Belging Party Trust. View New Window from Here ☑ Item I Item I

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.intell/indev.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 for federation metadata to file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: Federation metadata about the relying party manualy 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

🖬 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

Add Relying Party Trust	Wizard					
choose Access Control Policy						
eps	Choose an access control policy:					
Welcome	Name	Description				
Select Data Source	Permit everyone	Grant access to everyone.				
Specify Display Name	Permit everyone and require MFA	Grant access to everyone and requi				
Configure Certificate	Permit everyone and require MFA for specific group	Grant access to everyone and requi				
	Permit everyone and require MFA from extranet access	Grant access to the intranet users ar				
Configure URL	Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and requi				
Configure Identifiers	Permit everyone and require MFA, allow automatic device registr					
Choose Access Control	Permit everyone for intranet access	Grant access to the intranet users.				
Policy	Pamil enantin mun	Grant annaee to ceare of one or mor				
Ready to Add Trust						
Finish	Policy					
	Permit everyone					
	 I do not want to configure access control policies at this time. No application. 	user will be permitted access for this				
	< Prev	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

Nance	Iranaform	Rules				
The folk	owing tren	aforn rules sp	ofy the claim	s that will be sent	to the relying pa	rty.
Order	Rule N	ате		Issued	Cains	
						4
Add F	kule	Edt Rule	Bemove	Rule		

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 eloudd 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	~					
Incoming name ID format:	Unspecified	\sim					
Outgoing claim type:	Name ID	~					
Outgoing name ID format:	Outgoing name ID format:						
Pass through all claim values Replace an incoming claim value with a different outgoing claim value							
Incoming claim value:		_					
Outgoing claim value:	Browse						
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
122	People		Alasta Alasta
٢	Automation	~	Single Sign-on Access SSO (Single Sign-On) settings
۲	Settings		

3. Click Create SSO idP

SSO IdPs + Croste 150 MP	
	No SSO 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
ame - required
Demo SSO
nabled
ntity ID - required
https://ec2-54-79-24-127.ap-southeast-2.compute.amazonaws.com/adfs/services/trust
ingle Sign-On URL - required
https://ec2-54-79-24-127.ap-southeast-2.compute.amazonaws.com/adfs/ls
LO Endpoint URL - required
https://ec2-54-79-24-127.ap-southeast-2.compute.amazonaws.com/adfs/is
ame ID Format - required
Email address x *
509 Certificate - required
is can either be the full certificate or the fingerprint
uthnContextClassRef
No AuthnContext 👻
utiple choices are allowed
uthn Comparison - required
Exact
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 Assign and edit 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		
	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	le sign-on	

5. Click on Users and Groups

	intelliHR SSO Overview	
	«	
👢 Ov	verview	Properties
De	eployment Plan	Name ①
🗙 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 Si	ingle Sign-On with SAML		
d the co	onfiguration guide 🖉 for help integrating int	elliHR SSO.	
Ba	asic SAML Configuration		Ø
ld	lentifier (Entity ID)	Required	
Re	eply URL (Assertion Consumer Service URL)	Required	
Si	gn on URL	Optional	
Re	elay State	Optional	
10	ogout Url	Optional	

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

https://soo-demo.intellihrdev.net/saml2/metadata	efault () efault	
The default identifier will be the audience of the SAML response for IDP-initiated SSO	efault	
	efault	
https://so-demo.intellihrdev.net/saml2/metadata	efault	
Reply URL (Assertion Consumer Service URL) * ○ The default reply URL will be the destination in the SAML response for IDP-initiated SSO Inttps://soc-demo.intellihrdev.net/samt2/acs Sign on URL ○	efault	
The default reply URL will be the destination in the SAML response for IDP-initiated SSO		1
The default reply URL will be the destination in the SAML response for IDP-initiated SSO		101
The default reply URL will be the destination in the SAML response for IDP-initiated SSO		Î
D https://so-demo.intellihrdev.net/saml2/acs Sign on URL		Î
https://soo-demo.intellihrdev.net/samt2/acs		181
sign on URL O	0	TÊT
-		
-		
-		
https://sso-demo.intellihrdev.net/auth/login		
		~
Relay State 🕕		
Enter a relay state		
oqout Url 💮		
https://sso-demo.intellihrdev.net/auth/logout		

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

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

- <keydescriptor us<br="">-<x509data> -<x509certific MIIC8DCCA GWjdbUFfCl UAB5TyPUn</x509certific </x509data></keydescriptor>	ate> iigAwIBAgIQMKi6ZYyIg4pCMzc0rPCOijANBgkqhkiG9w0BAQsFADA0MTIwMAYDV0 BpRq+OłQnh2UDC0fd78jrcd+l0wf2jyYWHWEaOqij38vvLhhDyMs02+UQVyt0HF 155v4rnb0h40IDA0ABMA0GSGSI5D0DE6CwUAA4IBA0CIPw8tATDm15Fng5	QDEylNaWNyb3NvZnQgQX 2/19YfOEDNCCQoKUGPsAuc cknOK	p1cmUgRmVkZXJhdGVklFNTTyBDZXJ0a LKfY/Q0q5MbD9CAlYIn4PJnZJxhZ+lDcT	tvil94
pchVSsfpejn	16C3JsPOSnYfDmrUWFpefkTo9wxlaJHh09KY4N1vWJye0tpVsj+YmxCdRiJraPhCNj2 TpRbm8G+kCWunqQ0px8DkIj++7ZMdfi2IraxkklCvubTHHOVAI9AaJX0LmW1Ab0C	eg4LggWIn8fg10/l6ndrSjz00	I64OLHLDVMCA/g6Vo74aFrA2iIPrI6XYth IPXYRVV6x	1
tOK9xvv0uo <th>HvGPO5kvWmzkt1rkH72oNhs+oFBnEFuVooxXOdl3xHaYNn0iFnOw8HOVICZcDs3U cate></th> <th>J+Sn</th> <th></th> <th></th>	HvGPO5kvWmzkt1rkH72oNhs+oFBnEFuVooxXOdl3xHaYNn0iFnOw8HOVICZcDs3U cate>	J+Sn		
	Create SSO IdP			
	Name - required	\$333333333		
	Azure SSO Demo			
	Enabled			
	Entity ID - required	200000000		
	https://sts.windows.net/8edc0761-49d9-43aa-9dfc-13f00761405b/			
	Single Sign-On URL - required	Set up intelliHR SSO		
	https://login.microsoftonline.com/8edc0761-49d9-43aa-9dfc-13f00761405b/saml2	You'll need to configure the applicati	on to link with Azure AD. https://login.microsoftonline.com/8edc0761-	
		Azure AD Identifier	https://sts.windows.net/8edc0761-49d9-43a	
	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			
	Email address	ו 00000000		
	x509 Certificate - required			
	m			
		100000000		
	This can either be the full certificate or the fingerprint	000000000		
	AuthnContextClassRef			
	No AuthnContext			
	Multiple choices are allowed			
	Authn Comparison - required			
	Exact	 		
	Create SSO IdP	200000000		
	Create SSURP			

5. The user can now login via SSO



