Integrating Ideanote with ADFS

To setup Ideanote with ADFS please follow these steps.

1. Go to AD FS management and open the "Relying Party Trust Wizard".

%	AD FS	_ 🗆 X
翰 File Action View Window Help		_ 8 ×
	Add Relving Party Trust Wizard	
AD FS		lections
Welcome		Relying Party Trusts 🛛 🔺
Claims Claims Relying Authentice Configure MultiActor Authentice Configure MultiActor Authentice Conset Issuance Authoration Rules Ready to Add Trust Prish	Welcome to the Add Relying Party Trust Wizard This witsard will help you add a new relying party that to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions. The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.	Add Relying Party Trus Add Non-Claims-Awar View > New Window from Here Refresh Refresh Refresh Refresh Refresh Help deanote Test 2 Update from Federatio Edit Claim Rules Disable Properties Delete Help
Action: In progress	< Previous Stat Cancel	

2. Now enter the following URL in "Federation metadata address (host name or URL):"

https://api.ideanote.io/sso/saml/metadata.xml

\$	Add Relying Party Trust Wizard
Select Data Source	
Select Data Source Steps Select Data Source Select Data Source Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Select an option that this wizard will use to obtain data about this relying party: 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 its federation metadata address (host name or URL):
	< Previous Next > Cancel

3. Enter "Ideanote" as Display Name (or anything you want)

\$	Add Relying Party Trust Wizard	x
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	Ideanote	
Specify Display Name	Notes:	
Configure Multi-factor Authentication Now?		^
 Choose Issuance Authorization Rules 		
Ready to Add Trust		
• Finish		
	< Previous Next > Cancel	

4. Finish the "Add Relaying Party Trust Wizard" and open the "Edit Claim Rules" dialog.

\$			Edit C	Claim R	ules for	Ideanote	!	-		x
Issua	ance T	ransform Rules	Issuanc	e Authoriz	ation Rule	s Delegatio	n Authoriza	ation F	ules	
Th	ne follo	wing transform n	ules speci	ify the clai	ms that wi	ll be sent to th	ne relying p	arty.		
C	Order	Rule Name				Issued Clain	15			
									1	<u> </u>
										7
	Add R	ule Edit F	Rule	Remov	e Rule					
					0	Ж	Cancel		Арр	ly

5. Add a rule using the template "Send LDAP Attributes as Claims" and setup the following LDAP Attributes:

artment".
3

	Add Transform Claim Rule Wizard				
Configure Rule					
Configure Rule Steps Choose Rule Type Configure Claim Rule	You c which issuec Claim Send Rule t Active Mapp	an configure this rule to send the valu to extract LDAP attributes. Specify ho from the rule. rule name: LDAP Attributes as Claims emplate: Send LDAP Attributes as Cla fe store: a Directory ing of LDAP attributes to outgoing clai LDAP Attribute (Select or type to add more) E-Mail-Addresses Given-Name Surname Department	es of L www.the ims mtype: v v v v v v v	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be s: Outgoing Claim Type (Select or type to add more) E-Mail Address v Given Name v Sumame v Department v	

6. Next, add a new rule using the template "Transform an Incoming Claim". This rule has to transform incoming claim type "E-Mail Address" to outgoing claim type "Name ID: Email".

%	Add Transfo	orm Claim Rule Wizard	X		
Configure Rule					
Steps	You can configure this rule to also map an incoming claim v	map an incoming claim type to an outgoing alue to an outgoing claim value. Specify th	g claim type. As an option, you can e incoming claim type to map to the		
Configure Claim Rule	outgoing claim type and whet	her the claim value should be mapped to a	new claim value.		
	Claim rule name:				
	Transform Email Name ID				
	Rule template: Transform an	ncoming Claim			
	Incoming claim type:	E-Mail Address	¥		
	Incoming name ID format:	¥			
	Outgoing claim type:	Name ID 🗸			
	Outgoing name ID format:	Email	¥		
	Pass through all claim value	Jes			
	 Replace an incoming clair 	n value with a different outgoing claim value	e		
	Incoming claim value:				
	Outgoing claim value:		Browse		
	O Replace incoming e-mail s	uffix claims with a new e-mail suffix			
	New e-mail suffix:				
		Example: fabrikam.com			
		< Previous	s Finish Cancel		

7. Finally make sure that the AD FS supports "Form Authentication".

12	
翰 File Action View Window	Edit Global Authentication Policy
	Primary Multi-factor
 AD F3 ▷ III Service ⊿ III Trust Relationships 	users to have a choice of what method to authenticate with at sign in.
Claims Provider Trusts	authentication method on browsers that support Integrated Windows authentication. Extranet
 Attribute Stores Authentication Policies Per Relying Party Trust 	✓ Forms Authentication ○ Certificate Authentication
	Intranet Forms Authentication Windows Authentication
	Enable device authentication
	OK Cancel Apply

8. Now we need to link Ideanote to be using your AD FS as Identity Provider. First, download FederationMetadata.xml from the FederationMetadata URL of your intranet that looks something like this.

https://youintranet.com/FederationMetadata/2007-06/FederationMetadata.xml

9. Upload the FederationMetadata to SSO Settings in Ideanote or enter the values manually. Optionally enter an "Unauthorized Message" to show if something fails during single sign on.



Save