

Connect ADFS to SAML 2.0

General ADFS Setup - This procedure uses ADFS 3.0 and shows samlportal.example.com as the

ADFS website. Replace this with your ADFS website address.

Before you begin...

If you have Azure AD, please follow these instructions instead.

If you have ADFS 2.0, the navigation provided in these instructions may not be consistent with your ADFS interface.

Provide your ClearCompany Customer Success Manager with the following

information (if you have a metadata file for your organization, please send that to your IM or CSM -

this will give us the two items listed here).

- 1. IdP login URL
- 2. PEM encoded x.509 certificate
 - a. Log into the ADFS server and open the management console.
 - 1. Right-click Service and choose Edit Federation Service Properties...





a. Confirm that the General settings match your DNS entries and certificate names. Take note of the Federation Service Identifier, since that is used in the ClearCompany SAML 2.0 configuration settings.

	Federation Service Properties	×
General Feder	Organization Events ation Service display name:	
samlp	ortal.example.com	
Feder	ation Service name:	
samlp	ortal.example.com	
Exam Feder	ple: fs.fabrikam.com ation Service identifier:	
http://	/samlportal.example.com/adfs/services/trust	
Examj Web 1	ple: http://fs.fabrik.am.com/adfs/services/trust SSO lifetime: 480	
	OK Cancel Apply	

b. Browse to the certificates and export the Token-Signing certificate
 i. Right-click the certificate and select View Certificate ii.

Select the Details tab

- iii. Click **Copy to File...** the Certificate Export Wizard launches
- iv. Select Next

v. Ensure **No**, **do not export the private key** is selected, and then click **Next** vi. Select **DER encoded binary X.509 (.cer)** and then click **Next** vii. Select where you want to save the file and give it a name. Click **Next** viii. Select **Finish**

c. Give this X.509 Certificate in PEM format to ClearCompany along with the login url.

ADFS Relying Party Configuration

Here is where we will manually configure the relying party

 Navigate to SAML 2 Single Sign-on > Properties and verify that the SAML property Sign Authn Request (glide.authenticate.sso.saml2.require_signed_authnrequest) is not active.



- 2. Open the ADFS Management console and select Relying Party Trusts
- Select Add Relying Party trust from the top right corner of the window. The Add Wizard appears
 Click Start to begin
- 5. Select Import data about this relying party published online or on a local network

40 FS 2.0			_ 8 ×
File Action View W	indow Help		_18 ×
E Service	Madd Relying Party Trust	Wizard	×
Endpoints Certificates	Select Data Source		ng Party Trust
Claim Descriptions Trust Relationships Claims Provider Trus Relying Party Trus Attribute Stores	Skeps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers 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 online or on a local network. Federation metadata address (host name or URL): 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 expreted is federation metadata on a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: Browse Federation to manually input the necessary data about this relying party organization. Browse Import data about the relying party manually Browse Federation metadata file location: Browse Federation to manually input the necessary data about this relying party organization. Help	ow from Here
Action: In progress			
[] Start 🛜 🚠 🚨	/ @ 0 = 9		* 🏳 🖗 🎲 1:03 PM 💻

- Input the following URL: <u>https://api.clearcompany.com/v1/auth/sso/saml/sp/metadata</u> and click Next.
- 7. Move on to setting up the Relying Party Claim Rules (instructions on the next page) 8. *If you wish to set this up manually, you can use the following instructions:*
 - a. Select ADFS 3.0 Profile
 - b. Do not select a token encryption certificate
 - i. It will use the certificate that is defined on the service that has already been exported. Defining a certificate here will prevent proper communication with ClearCompany
 - c. Do not enable any settings on the Configure URL



The Talent Maximization Company

- d. Enter the ClearCompany website to which you connected as the Relying Party trust identifier. In this case use https://api.clearcompany.com and click Add
- e. Permit all users to access this relying party
- f. Click Next and clear the Open the Claims when this finishes check box.
- g. Close this page the new relying party trust appears in the window
- h. Right click on the relying party trust and select Properties
- i. Browse to the Advanced tab and set the **Secure hash algorithm** to 'SHA1' or 'SHA-256'
- j. Browse to the Endpoints tab and add a **SAML Assertion Consumer Service (ACS URL)** with a **POST** binding and a URL of <u>https://api.clearcompany.com/v1/auth/sso/saml</u>

ADFS Relying Party Claim Rules

Edit the Claim rules to enable proper communication with ClearCompany. We need to set up two rules.

- 1. Right-click on the relying party trust and select Edit Claim Rules
- 2. On the Issuance Transform Rules tab select Add Rules
- 3. Select Send LDAP Attribute as Claims as the claims rule template to use.
- 4. Give the claim a name such as Get LDAP Attributes
- 5. Set the Attribute Store to **Active Directory**, the LDAP Attribute to **E-Mail Addresses**, and the Outgoing Claim Type to **E-Mail Address**.

	Edit Rule	- Get Attribute
You c which issued	an configure this rule to send the values of L to extract LDAP attributes. Specify how the d from the rule.	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be
Get ó	nue name. Nrikule	
Rule	remplater Send LDAP Attributes as Claims	
Activa	a Directory	
Марр	ing of LDAP attributes to outgoing claim type	£
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
۲	E-Mail-Addresses 🗸 🗸	E-Mail.Address
*	×	



- 6. Select Finish
- 7. Select Add Rule
- 8. Select **Transform an Incoming Claim** as the claim rule template to use.
- 9. Give it a name such as Email to Name ID
 - a. Incoming claim type should be **E-Mail Address** (it must match the **Outgoing Claim Type in rule #1**. The Outgoing claim type is **Name ID** (this is requested in ClearCompany policy

and the Outgoing name ID format is **Unspecified**

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
(or Email). Pass through all claim values and click Finish .

You can configure this rule to also map an incoming claim v outgoing claim type and whe	o map an incoming claim type to an outgoing cla value to an outgoing claim value. Specify the inc ther the claim value should be mapped to a new	im type. As an op coming claim type v claim value.	ption, you can a to map to the
Claim rule name:			
Email to NameID			
Rule template: Transform an	Incoming Claim		
Incoming claim type:	E-Mail Address	~	
Incoming name ID format:	Unspecified	~	
Outgoing claim type:	Name ID	~	
Uutgoing name ID format: Pass through all claim val Replace an incoming clai	Email	*	
 Pass through all claim val Replace an incoming claim value Dutgoing claim value 	Email	Biowse	
Pass through all claim val Pass through all claim val Replace an incoming claim value: Dutgoing claim value: Dutgoing claim value: Paplace incoming e-mail	Email lues in value with a different outgoing claim value	Biowse	
 Pass through all claim val Replace an incoming claim value. Dutgoing claim value. Replace incoming e-mail New e-mail suffice 	Email Les im value with a different outgoing claim value suffix claims with a new e-mail suffix	•	



Logging into ClearCompany using SSO

- 1. SP-Initiated Login
 - a. Open your browser and navigate to https://[shortname].clearcompany.com
 - b. This will automatically redirect you to your Identity Provider Log-in page.



c. Once you log in using these credentials, if you are not already signed into your server, your browser will redirect you to your logged-in ClearCompany home page.

2. IdP-Initiated Login

- a. For some IdPs, you are able to access the ClearCompany platform from your server's site.
- b. From your IdP site, click on the ClearCompany tile or link (if available) this will redirect you automatically to ClearCompany.

Things to Note

1. Usernames

- a. In ClearCompany the value we use for matching user identification is the Employee Username this can be found by going to Tools \rightarrow Setup \rightarrow Users.
- b. In ADFS if you used the Relying Party Claim Rules setup instructions above, the value that will be used to match is the employee's Email Address within your Active Directory.

2. Email Links

- a. If your team needs to access the system through email links for example, an approval to an Offer Letter - this should still work. The user will click on the link and go through the authentication process and be brought right to the Offer Letter Approval Page
- b. Some clients have reported that they have to click this link once to go through the authentication process, and then they must click it again to be brought to the Offer Letter page. This typically happens because some IdPs cannot properly pass on a RelayState. If this occurs, please check if your IdP allows passing a RelayState.