ClearCo.

The Talent Maximization Company

# 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.*

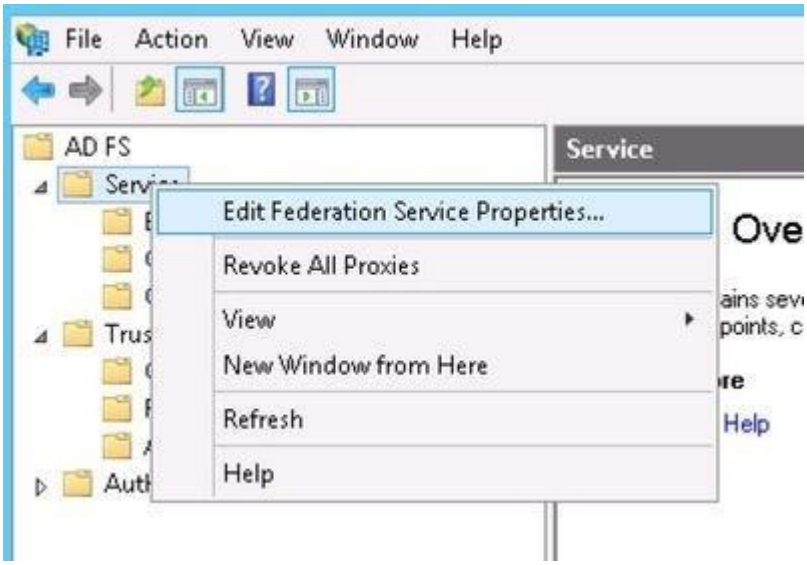
Before you begin…

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

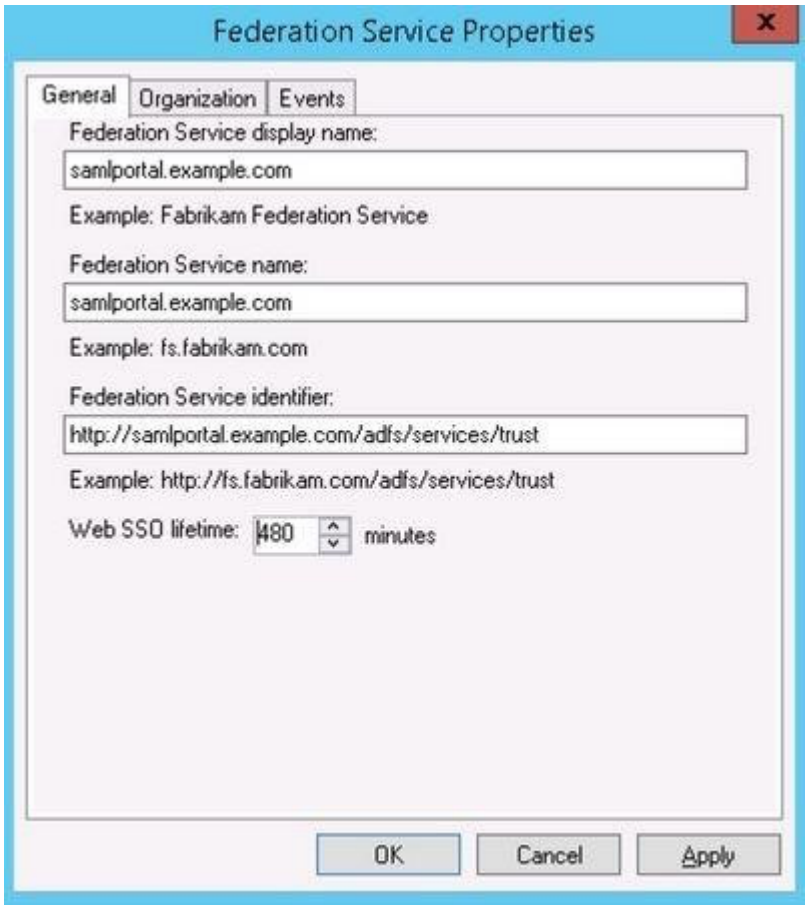
If you have ADFS 2.0, the navigation provided in these instructions may not be consistent with your ADFS interface.

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.




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**

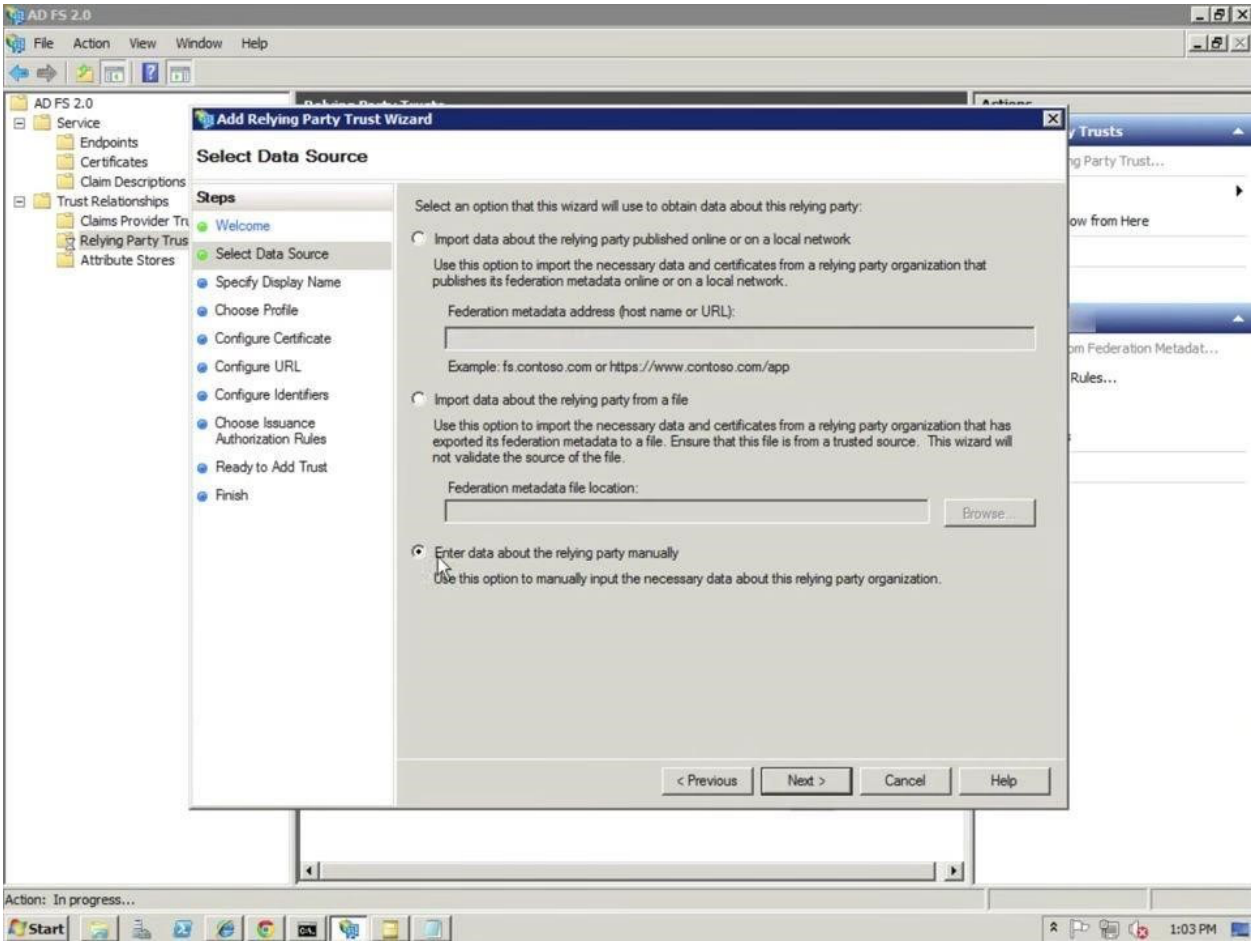
c. Give this X.509 Certificate in PEM format to ClearCompany along with the login url.

## ADFS Relying Party Configuration

Here is where we will manually configure the relying party

1. 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**
3. Select **Add Relying Party trust** from the top right corner of the window. The Add Wizard appears
4. Click **Start** to begin
5. Select **Import data about this relying party published online or on a local network**



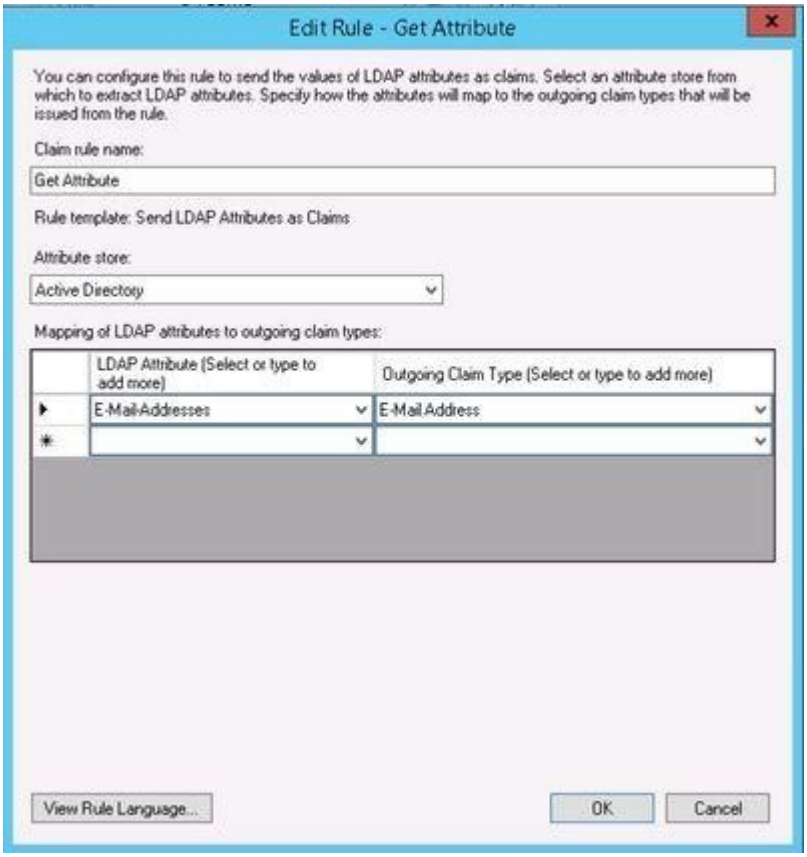

6. Input the following URL: https://api.clearcompany.com/v1/auth/sso/saml/sp/metadata and click Next.
7. Move on to setting up the Relying Party Claim Rules (instructions on the next page) 8. *If you wish to set this up manually, you can use the following instructions:*
    a. Select **ADFS 3.0 Profile**
    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**

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 https://api.clearcompany.com/v1/auth/sso/saml

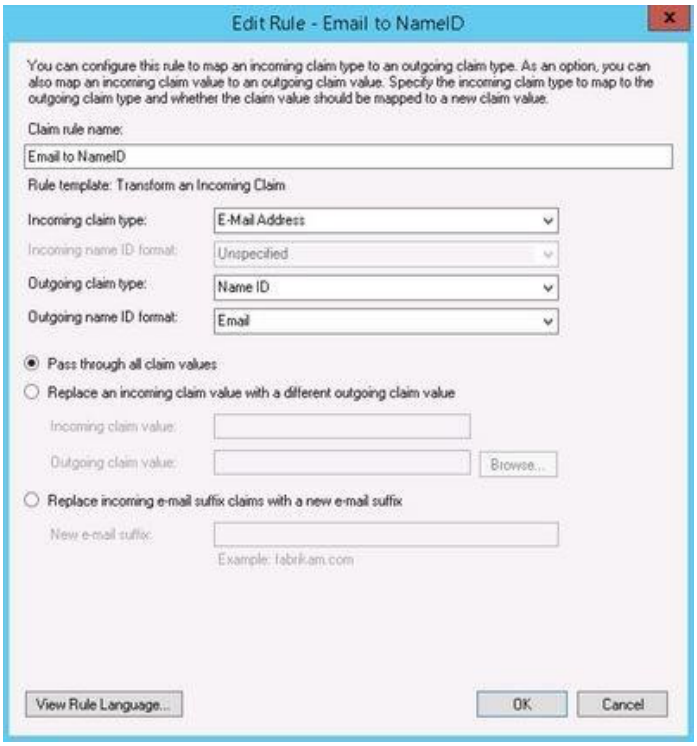
## ADFS Relying Party Claim Rules

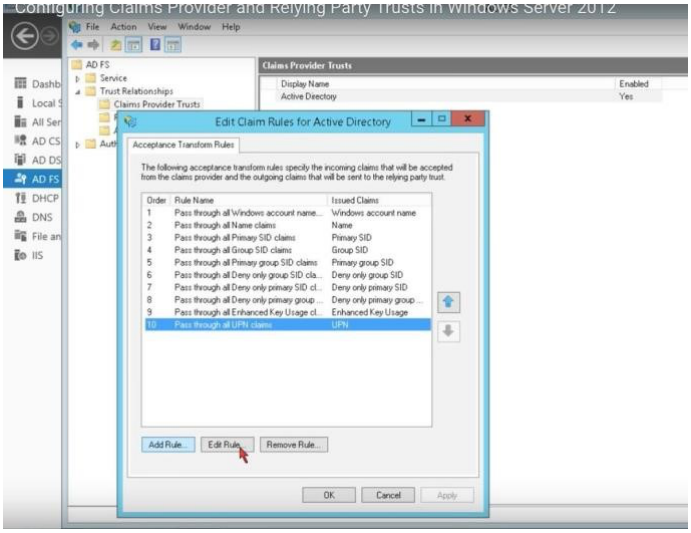
Edit the Claim rules to enable proper communication with ClearCompany. We need to set up two rules.

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.**



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




## 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 → Setup → 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.