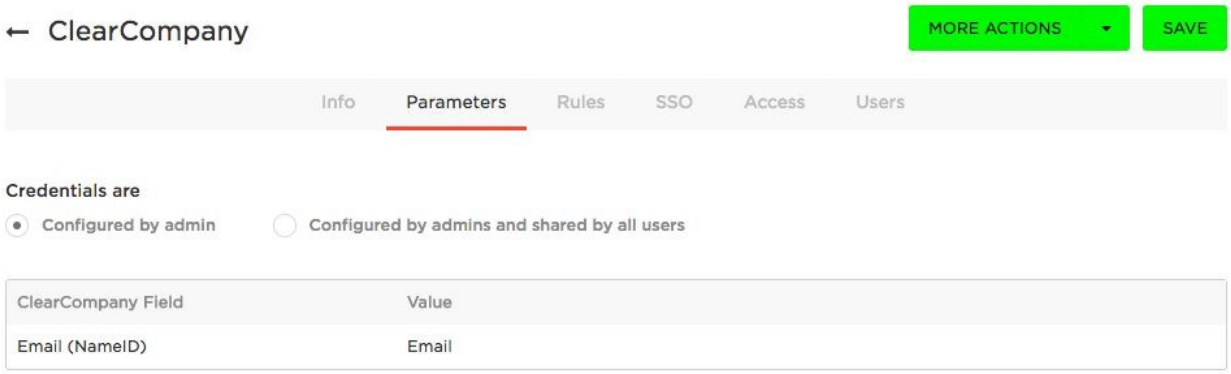
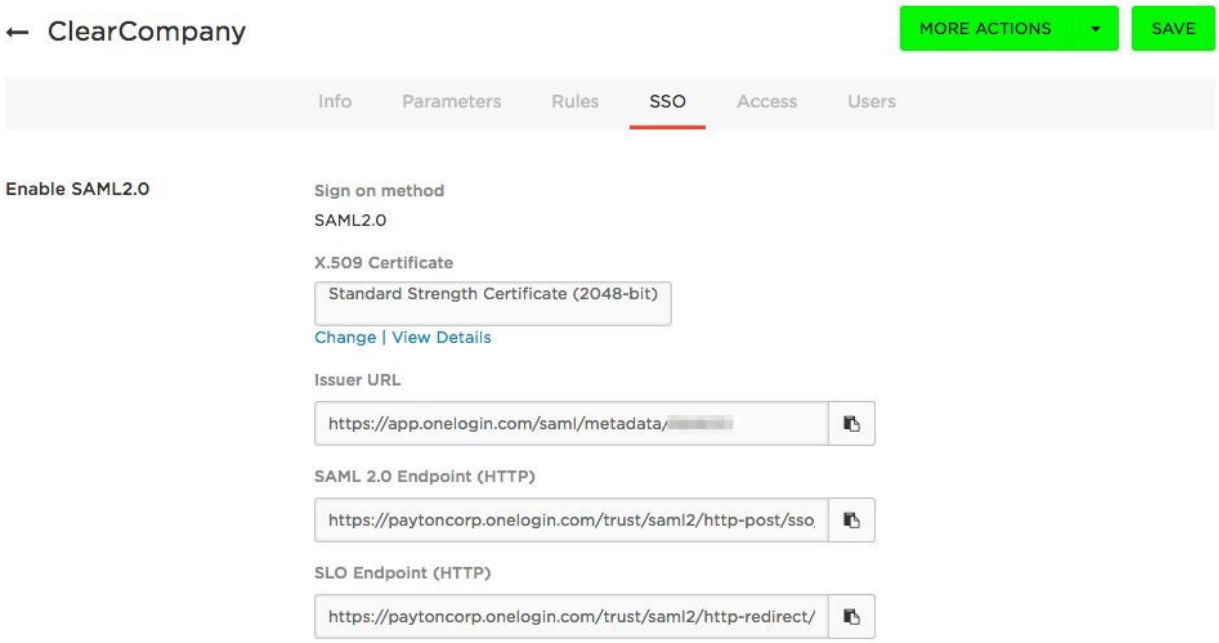
SSO Setup for OneLogin

1. OneLogin Configuration Instructions (from https://support.onelogin.com/hc/en-us/articles/210943203-Configuring-SAML-For-ClearCompany)
    a. Log into OneLogin as an Admin and go to **Apps** → **Add Apps**
    b. Search for and select the *ClearCompany SAML* connector
        i. The initial **Configuration** tab appears
    c. Click **Save** to add the app to your Company Apps and display additional configuration tabs.
        i. The **Info** tab appears
    d. Go to the **Parameters** tab and map ClearCompany attributes to OneLogin attributes
        i. In most cases, you should keep the **Configured by admin** default. For more information, see Setting Credential Configuration Options.
        ii. For most implementations, you can accept the default attribute mappings. Ensure that the ClearCompany field **Email (NameID)** is set to *Email.*



        iii. Click **Save** to save your changes on the **Parameters** tab.
    e. Go to the **SSO** tab to obtain the **SAML 2.0 Endpoint (HTTP)** and the **X.509 Certificate** file that you must send to your ClearCompany representative to configure SAML SSO



i. Copy the **SAML 2.0 Endpoint (HTTP)** value found on the SSO tab.
ii. Obtain the **X.509 Certificate** by selecting View Details. Then select **Download** to download the certificate. iii. Send both the **SAML 2.0 Endpoint (HTTP)** and the **X.509 Certificate** file to your ClearCompany representative. The team will enable SAML SSO for you when you are ready to test.

f. On the OneLogin **Access** tab, assign the OneLogin roles that should have access to ClearCompany and provide any app security policy that you want to apply to ClearCompany
   i. You can also go to **Users** → **All Users** to add the app to individual user accounts

g. Click **Save**

2. Testing
   a. Ensure that ClearCompany has received and processed your SAML 2.0 Endpoint (HTTP) and IdP Metadata file
   b. Your SAML connection will not work until ClearCompany has processed this information from you
   c. Ensure that you have user accounts in both OneLogin and ClearCompany that use the same email as the username
   d. You can create a test user, or you can use your own account if you choose

e. Make sure you are logged out of ClearCompany.

i. Identity Provider (OneLogin)-initiated login
   1. Log into OneLogin as an admin and give the test user access to the ClearCompany app in OneLogin (see step 8 above)
   2. Log into OneLogin as the test user
   3. Click the ClearCompany icon on your OneLogin dashboard
   4. If you are able to access ClearCompany, then this test is successful

ii. Service Provider (ClearCompany)-initiated login
   1. Ensure you are logged out of ClearCompany and OneLogin
   2. Navigate to https://[shortname].clearcompany.com
   3. Once redirected, enter your OneLogin credentials and click **Submit**
   4. If you have been logged into ClearCompany, then this test is successful.

3. Things to Note:

a. Usernames

i. In ClearCompany - the value we use for matching user identification is the Employee Username - this can be found by going to Tools → Setup → Users ii. In OneLogin - the value they use for matching user identification is the user's email address

iii. In short, the email address entered for a user in OneLogin must be the same value as the ClearCompany Employee Username

b. Email Links

i. 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

ii. 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.