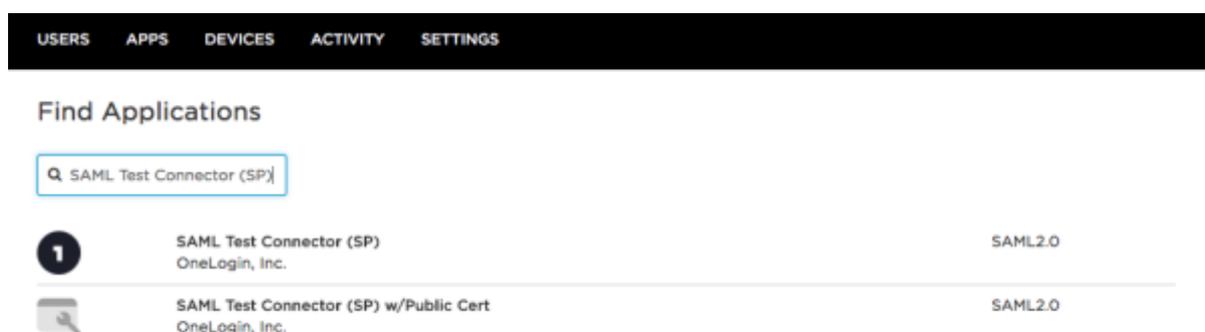




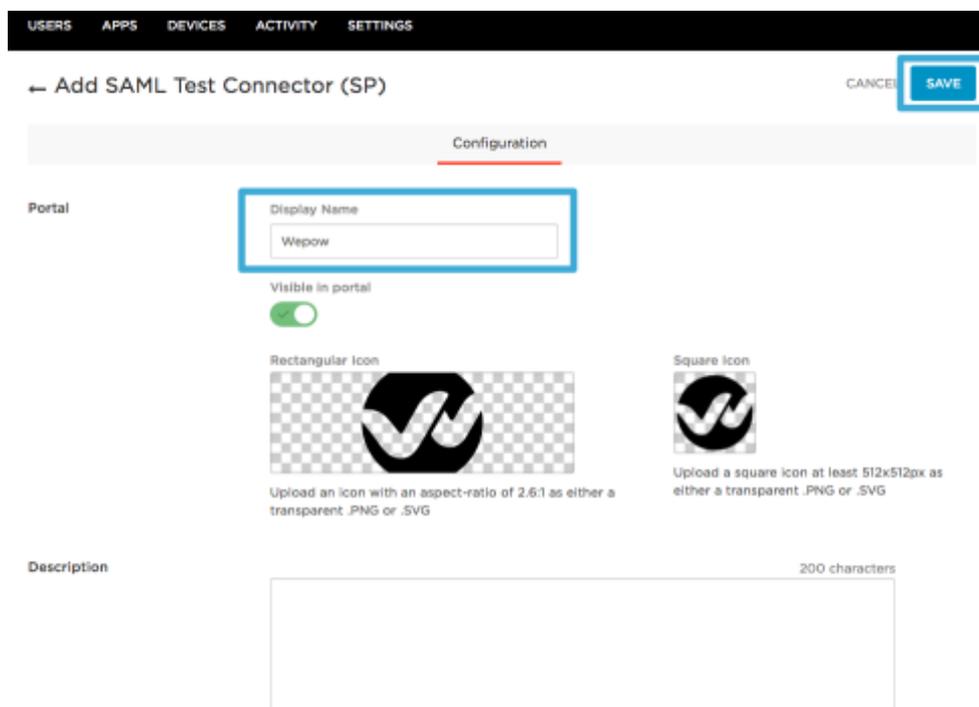
OneLogin is a single sign-on provider, which makes it easy to manage your application logins and permissions.

In OneLogin

1. Click on the Apps tab and select the option "Add Apps." In the new page, search for the application **SAML Test Connector (SP)**



2. After selecting the app, configure the Connector. Add the name for your app under the "Display Name" field.



* Enter the fields information with the below values:



- Audience: wepowapp.com
- Recipient: wepowapp.com
- ACS (Consumer) URL Validator:
^https://\wepowaccountsubdomain\.wepowapp\.com\sso\saml\consume
- ACS (Consumer) URL:
https://wepowaccountsubdomain.wepowapp.com/sso/saml/consume
- Single Logout URL: https://wepowaccountsubdomain.wepowapp.com/en/logout
- Login URL: https://wepowaccountsubdomain.wepowapp.com/sso/saml/init

Once all the information is entered, click "Save."

3. The next section to update is "Parameters." Depending on the quantity of user roles and teams, the values of the parameters can be added. These are the values to add:

- first_name
- last_name
- is_owner (custom)



- wepow_role_1 (number added depending on the total users added to the account) (custom)
- wepow_team_1 (number added depending on the total teams added to the account) (custom)

* The only value by default is the email.

Check this [guide](#) to create custom fields

USERS APPS DEVICES ACTIVITY SETTINGS

← SAML Test Connector (SP) MORE ACTIONS SAVE

Info Configuration **Parameters** Rules SSO Access Users Privileges

Credentials are

Configured by admin Configured by admins and shared by all users

SAML Test Connector (SP) Field	Value	Add parameter
Email (NameID)	Email	
first_name	First Name	custom parameter
is_owner	wepow_is_owner (Custom)	custom parameter
last_name	Last Name	custom parameter
wepow_role_1	wepow_role_1 (Custom)	custom parameter
wepow_team_1	wepow_team_1 (Custom)	custom parameter

Add the field name with the values mentioned above and check the "Flags" box

New Field

Field name

This is the name of the field in the application's API

Flags Include in SAML assertion

CANCEL SAVE



Click to edit the information from the parameter.

← SAML Test Connector (SP) MORE ACTIONS SAVE

Info Configuration **Parameters** Rules SSO Access Users Privileges

Credentials are
 Configured by admin Configured by admins and shared by all users

SAML Test Connector (SP) Field	Value		Add parameter
Email (NameID)	Email		
is_owner	- No default -		custom parameter

Edit the "value" field select the custom value created.

Edit Field Is_owner

Name: is_owner

Value:

Flags:

- Username
- userPrincipalName
- wepow_is_owner (Custom)
- wepow_role_1 (Custom)
- wepow_team_1 (Custom)

SAVE



4. Once the parameters are configured it is necessary to create your users, teams, and [mappings](#)

In Wepow

From OneLogin copy the information from the tab "SSO" copy the "SAML 2.0 Endpoint (HTTP)" and "SLO Endpoint (HTTP)" URLs and paste them in the Wepow app under the Single Sign-on section

The screenshot shows the configuration page for a SAML Test Connector (SP) in Wepow. The page has a dark navigation bar at the top with 'USERS', 'APPS', 'DEVICES', 'ACTIVITY', and 'SETTINGS'. Below this is a breadcrumb '← SAML Test Connector (SP)' and two buttons: 'MORE ACTIONS' and 'SAVE'. A horizontal menu below the breadcrumb includes 'Info', 'Configuration', 'Parameters', 'Rules', 'SSO' (highlighted with a red underline), 'Access', 'Users', and 'Privileges'. The main content area is titled 'Enable SAML2.0' and contains several fields: 'Sign on method' is set to 'SAML2.0'; 'X.509 Certificate' is set to 'Standard Strength Certificate (2048-bit)' with a 'Change | View Details' link; 'SAML Signature Algorithm' is set to 'SHA-1'; 'Issuer URL' is 'https://app.onelogin.com/saml/metadata/679307'; 'SAML 2.0 Endpoint (HTTP)' is 'https://wepowtest-dev.onelogin.com/trust/saml2/http-post'; and 'SLO Endpoint (HTTP)' is 'https://wepowtest-dev.onelogin.com/trust/saml2/http-redin'. At the bottom, there is an 'Assumed Sign-in' section with a checkbox 'Allow assumed users to sign into this app' which is currently unchecked. Below the checkbox is a paragraph of explanatory text.



The screenshot shows the 'Single Sign-on' configuration page in Wepow. The left sidebar contains navigation menus for 'My Preferences', 'Team Settings', and 'Organization Settings'. The main content area is titled 'Single Sign-on' and features three radio button options: 'Deactivate single sign-on', 'Social Login', and 'SAML 2.0'. The 'SAML 2.0' option is selected. Below these options are several input fields: 'X.509 Certificate' (containing a long alphanumeric string), 'SAML 2.0 Endpoint (HTTP)', 'SLO Endpoint (HTTP)', 'Single Sign-on URL', and 'Single Logout URL'. At the bottom, there are two checked checkboxes: 'Allow email/password login' and 'Auto-provision users and teams'. A green 'Save' button is located at the bottom right of the configuration area.

Copy the certificate X.509 from OneLogin

The screenshot shows the 'SAML Test Connector (SP)' configuration page in OneLogin. The top navigation bar includes 'USERS', 'APPS', 'DEVICES', 'ACTIVITY', and 'SETTINGS'. The page title is 'SAML Test Connector (SP)' with 'MORE ACTIONS' and 'SAVE' buttons. Below the title is a tabbed interface with 'Info', 'Configuration', 'Parameters', 'Rules', 'SSO', 'Access', 'Users', and 'Privileges'. The 'SSO' tab is active. The main content area is titled 'Enable SAML2.0' and includes a 'Sign on method' section with a dropdown menu set to 'SAML2.0'. Below this, there are three certificate options: 'X.509 Certificate', 'Standard Strength Certificate (2048-bit)', and 'Change | View Details'. The 'X.509 Certificate' option is highlighted with a blue box and a blue arrow. Below the certificate options is a 'SAML signature Algorithm' dropdown set to 'SHA-1'. Further down are input fields for 'Issuer URL', 'SAML 2.0 Endpoint (HTTP)', and 'SLO Endpoint (HTTP)'. At the bottom, there is an 'Assumed Sign-in' section with a checkbox for 'Allow assumed users to sign into this app' and a descriptive paragraph.



Copy the certificate and paste it in the X.509 Certificate section in the Wepow App.

← Standard Strength Certificate (2048-bit) DELETE SAVE

Key length: 2048-bit

SHA fingerprint: SHA1 72:89:E2:EF:E7:00:2F:9D:82:2B:B184:FC:AC:E4:00:AB: [copy]

X.509 Certificate [copy]

```
-----BEGIN CERTIFICATE-----
MIIEETCCAmgFAwIBAgIUJSJKNPAnfmMBTA3BBH2+uG6j1UwDQYJKoZIhvcNAQEF
BQAwVjELMAkGA1UEBmMCVWx0JAMBgNVBAQoMBXkxOG93MRUwEwYDVoQLDAsPbmVM
b2dpb1BjZFAxIDAsBgNVBAMMF09uZUxvZ2luEFY291bnQgMTEwMjU3MzB4ODTE3
MDEwOTIwMDg3NFo0TlYMDiMDUwMDg3NFowVjELMAkGA1UEBmMCVWx0JAMBgNV
BAoMBXkxOG93MRUwEwYDVoQLDAsPbmVMb2dpb1BjZFAxIDAsBgNVBAMMF09uZUxv
Z2luEFY291bnQgMTEwMjU3MzB4ODTE3MDEwOTIwMDg3NFo0TlYMDiMDUwMDg3NFow
AQEAWidA4c8F7dIG4gQ2pPGGBiCov1yh93MWMhOyy2uFbdm4MBIB0yluzg9+
Ojxf7seyvocISEJvl0+7AOIv7U5w3Uz3jge1Miw23CFG2oC+Imtyoox7opl
dCABwOX4CAI2EzP+yf8osLpyRl2I7F3UmdNXPyTtVY3vRBPYKgmXN+LsCeYoL
KB+gT1qyGozrWW/VOBm59jnh2jmEGBlaoV3FPqHPJ5GmgeQXhoyZKbOA+52dR
jQbqBGeOVsA2SAU7nXu4uZLp1gt2nbAq3oxJgd1XP16HGdLXjnlUZsUP6AWdf
rtwAzmjh8NbOcvfJuxE3QEIQDAQABo4rWMIHTMAwGA1UdEwEBwQCMAAAwHQYD
VR0BBYEFlxG3w25Pyy2XWVY5VwPka4RRBmIGTbGNNVHSMegYowgYIAFlxG3w2
5Pyy2XWVY5VwPka4RRBmIGTbGNNVHSMegYowgYIAFlxG3w25Pyy2XWVY5VwPka4
b3vudCAXMTAyNtoCFEIS7hwJ35AU7QnWQR9vnuo9VMM4GA1UdDwEBAwQEAWH
gDANBgkqhkiG9w0BAQUFAAOCAQEAbN0Xsho1f89fbcf+098D8RcHrHy4tuC9tzA
2RnYskumLr3oYDwIn+XyaloP8chsrp8VRdZ45WBjraCTaH-Vr8Aasa9HWE
WVYAUZ91eWlO7hVWenR2VbC7kz9hmla2jHHe1A982547ZBv7G6pN07qk0
D7YxUjT0qSLQCMqXbfrK54wVJ21VnTgkdwN30nSaa7W9uPwhLFT
DoCclW8qLUEXvprSKB7TA9PRt49u+3NjmsOtrngyZ2W0gASAYQ8zaoO0D
nhNyAtoemS1eeRR02lbt14+EBmj5OaCqFQ+tz8tK0k6emg==
-----END CERTIFICATE-----
```

X.509 PEM DOWNLOAD

Apps using this certificate

- SAML Test Connector (...)
- WepowTest

SAML 2.0

Wepow can be configured for SSO by Identity Providers such as OneLogin, Okta, Ping Identity and others using SAML 2.0 protocol.

X.509 Certificate [copy]

```
-----BEGIN CERTIFICATE-----
MIIEETCCAmgFAwIBAgIUJSJKNPAnfmMBTA3BBH2+uG6j1UwDQYJKoZIhvcNAQEF
BQAwVjELMAkGA1UEBmMCVWx0JAMBgNVBAQoMBXkxOG93MRUwEwYDVoQLDAsPbmVM
b2dpb1BjZFAxIDAsBgNVBAMMF09uZUxvZ2luEFY291bnQgMTEwMjU3MzB4ODTE3
MDEwOTIwMDg3NFo0TlYMDiMDUwMDg3NFowVjELMAkGA1UEBmMCVWx0JAMBgNV
BAoMBXkxOG93MRUwEwYDVoQLDAsPbmVMb2dpb1BjZFAxIDAsBgNVBAMMF09uZUxv
Z2luEFY291bnQgMTEwMjU3MzB4ODTE3MDEwOTIwMDg3NFo0TlYMDiMDUwMDg3NFow
AQEAWidA4c8F7dIG4gQ2pPGGBiCov1yh93MWMhOyy2uFbdm4MBIB0yluzg9+
Ojxf7seyvocISEJvl0+7AOIv7U5w3Uz3jge1Miw23CFG2oC+Imtyoox7opl
dCABwOX4CAI2EzP+yf8osLpyRl2I7F3UmdNXPyTtVY3vRBPYKgmXN+LsCeYoL
KB+gT1qyGozrWW/VOBm59jnh2jmEGBlaoV3FPqHPJ5GmgeQXhoyZKbOA+52dR
jQbqBGeOVsA2SAU7nXu4uZLp1gt2nbAq3oxJgd1XP16HGdLXjnlUZsUP6AWdf
rtwAzmjh8NbOcvfJuxE3QEIQDAQABo4rWMIHTMAwGA1UdEwEBwQCMAAAwHQYD
VR0BBYEFlxG3w25Pyy2XWVY5VwPka4RRBmIGTbGNNVHSMegYowgYIAFlxG3w2
5Pyy2XWVY5VwPka4RRBmIGTbGNNVHSMegYowgYIAFlxG3w25Pyy2XWVY5VwPka4
b3vudCAXMTAyNtoCFEIS7hwJ35AU7QnWQR9vnuo9VMM4GA1UdDwEBAwQEAWH
gDANBgkqhkiG9w0BAQUFAAOCAQEAbN0Xsho1f89fbcf+098D8RcHrHy4tuC9tzA
2RnYskumLr3oYDwIn+XyaloP8chsrp8VRdZ45WBjraCTaH-Vr8Aasa9HWE
WVYAUZ91eWlO7hVWenR2VbC7kz9hmla2jHHe1A982547ZBv7G6pN07qk0
D7YxUjT0qSLQCMqXbfrK54wVJ21VnTgkdwN30nSaa7W9uPwhLFT
DoCclW8qLUEXvprSKB7TA9PRt49u+3NjmsOtrngyZ2W0gASAYQ8zaoO0D
nhNyAtoemS1eeRR02lbt14+EBmj5OaCqFQ+tz8tK0k6emg==
-----END CERTIFICATE-----
```

SAML 2.0 Endpoint (HTTP)

SLO Endpoint (HTTP)

Single Sign-on URL

Single Logout URL

Allow email/password login
Turn this off when you have completed testing login via your identity Provider.

Auto-provision users and teams
Automatically creates users and teams that match those on your identity Provider

Save



If "Auto-provision" is enabled, users should be created from OneLogin.

Thank you for using the Wepow Help Center! Our goal is to provide you with excellent customer service, and improve your experience when applying for a new job online!