SAML Server Setup (Service Provider)

1. Set up the web.config
2. Import the user’s metadata file using the Import Tool
3. Update the server’s saml.config file
4. Copy the user’s .cer file
5. Setup WMJ system settings

Notes:
The saml config file and all the certificates should all be backed up.

DNS
You will need a DNS entry for SAML users to use. This is separate from the Workamajig DNS entry that is normally used.

So, you could have classic.workamjig.com for classic use and saml.workamajig.com for SAML use.

One thing to note though, links in emails generated out of Workamajig will link to the SAML URL.

Meta data
Your identity provider should be able to generate a meta-data file that we'll need to then use that file to configure the Workamajig SAML configuration file.
You will need to provide them with these two pieces of information:
Entity ID:
ACS URL:

Here is an example of what we would use if you were hosted with us:
Entity ID: https://www.YOUR_DOMAIN.com
ACS URL: https://YOUR_SUB_DOMAIN.workamajig.com/platinum/sso/SAMLService.aspx

SAML Configuration
We have a tool we use to import the meta-data so one you have it, email it to support and we can setup the SAML config file and send it back to you

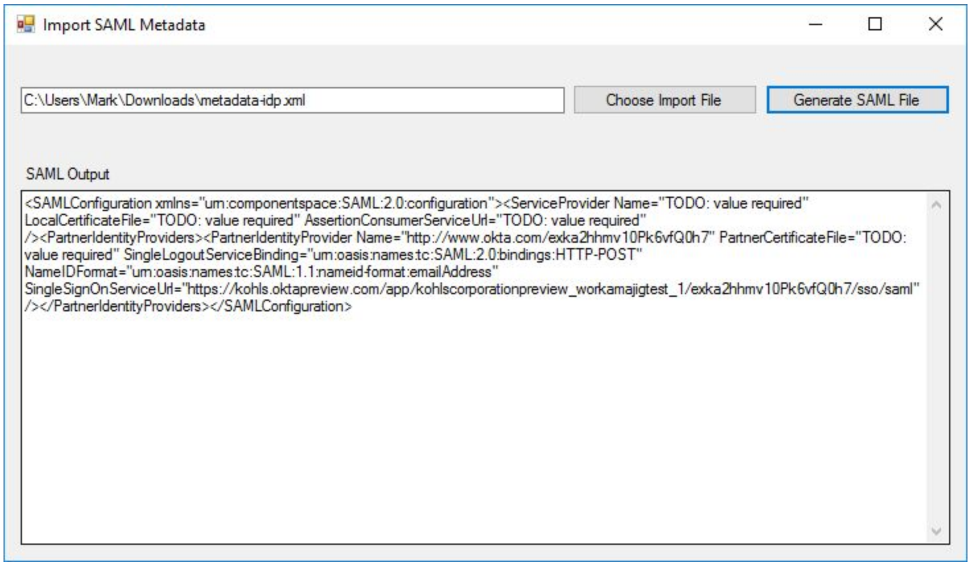
saml.config

The saml.config file is located in the WJAPP/sso folder.

User will need to provide meta data from their Identity Provider (IdP). The metadata file (in the form of an .xml file) will contain SAML attributes and their certificate.

Use the SAMLImportMetaData tool to generate the client's <PartnerIdentityProvider> node for the saml.config and extract the certificate into a separate .cer file.

1. Select the file to import
2. Generate the SAML File



C:\Users\Mark\Downloads\metadata-idp.xml

```
<SAMLConfiguration xmlns="urn:componentspace:SAML:2.0:configuration"><ServiceProvider Name="TODO: value required"
LocalCertificateFile="TODO: value required" AssertionConsumerServiceUrl="TODO: value required"
/><PartnerIdentityProviders><PartnerIdentityProvider Name="http://www.okta.com/exka2hhmv10Pk6vfQ0h7" PartnerCertificateFile="TODO:
value required" SingleLogoutServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
NameIDFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
SingleSignOnServiceUrl="https://kohls.oktapreview.com/app/kohlscorporationpreview_workamajigtest_1/exka2hhmv10Pk6vfQ0h7/sso/saml"
/></PartnerIdentityProviders></SAMLConfiguration>
```

1. Add the <PartnerIdentityProvider> information from the output window to the <PartnerIdentityProviders> in the saml.config file on the server.
2. Copy the .cer file to the server's WJAPP/sso folder
3. Edit the PartnerCertificateFile attribute of the <PartnerIdentityProvider> node to point to the .cer file.
   For example: PartnerCertificateFile="platinum\sso\newFile.cer"

Warning
The saml.config file must be a valid XML file. If not, SAML authentication will not work for any client on the server using it.

web.config

Modify the existing <sessionState> node to enable cookies. This is required by the SAML component.

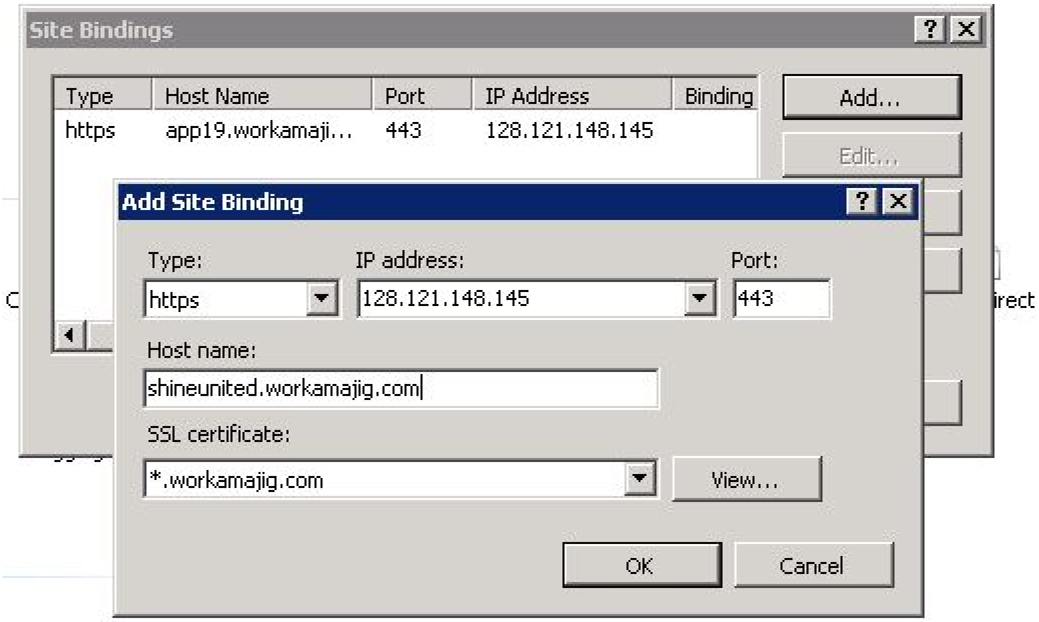
```
<sessionState mode="InProc" />
```

Add these two lines to the <appSettings> node

```
<!-- the prefix of the server. for example app1 -->
<!-- requests containing the NonSSOPrefix will be ignored by the SAML component -->
<add key="NonSSOPrefix" value="app" />

<!-- The relative or absolute path of the SAML configuration file. -->
<add key="SAMLConfigFile" value="C:Workamajig\web\WJAPP\saml.config"/>
```

Server Bindings



Site Bindings

Type	Host Name	Port	IP Address	Binding
https	app19.workamaji...	443	128.121.148.145	

Add Site Binding

Type: https

IP address: 128.121.148.145

Port: 443

Host name: shineunited.workamajig.com

SSL certificate: *.workamajig.com

Logging:
Normal WMJ SAML debug info is stored in the **webDebug.log**

To enable extended logging edit the web config and add this editing the **PATH.** This will enable all the requests and responses.

```
 </system.webServer>

            <system.diagnostics>
               <trace autoflush="true">
                  <listeners>
                      <add name="TextWriter"/>
                 </listeners>
               </trace>
               <sources>
                  <source name="ComponentSpace.SAML2" switchValue="Verbose">
                      <listeners>
                        <add name="TextWriter"/>
                     </listeners>
              </source>
            </sources>
            <sharedListeners>
              <add name="TextWriter"
                      type="System.Diagnostics.TextWriterTraceListener"
                      initializeData="C:\Workamajig\PATH HERE\log\idp.log"/>
             </sharedListeners>
          </system.diagnostics>
</configuration>
```

Setup WMJ/Platinum for SAML use

Use the Single Sign On (SSO) options to configure SAML.

- **URL Prefix*** - The prefix of the URL. For example, if the user WMJ URL is https://abc.workamajig.com, the prefix would be abc
    - The prefix must be different than the prefix specified in the web.config file.

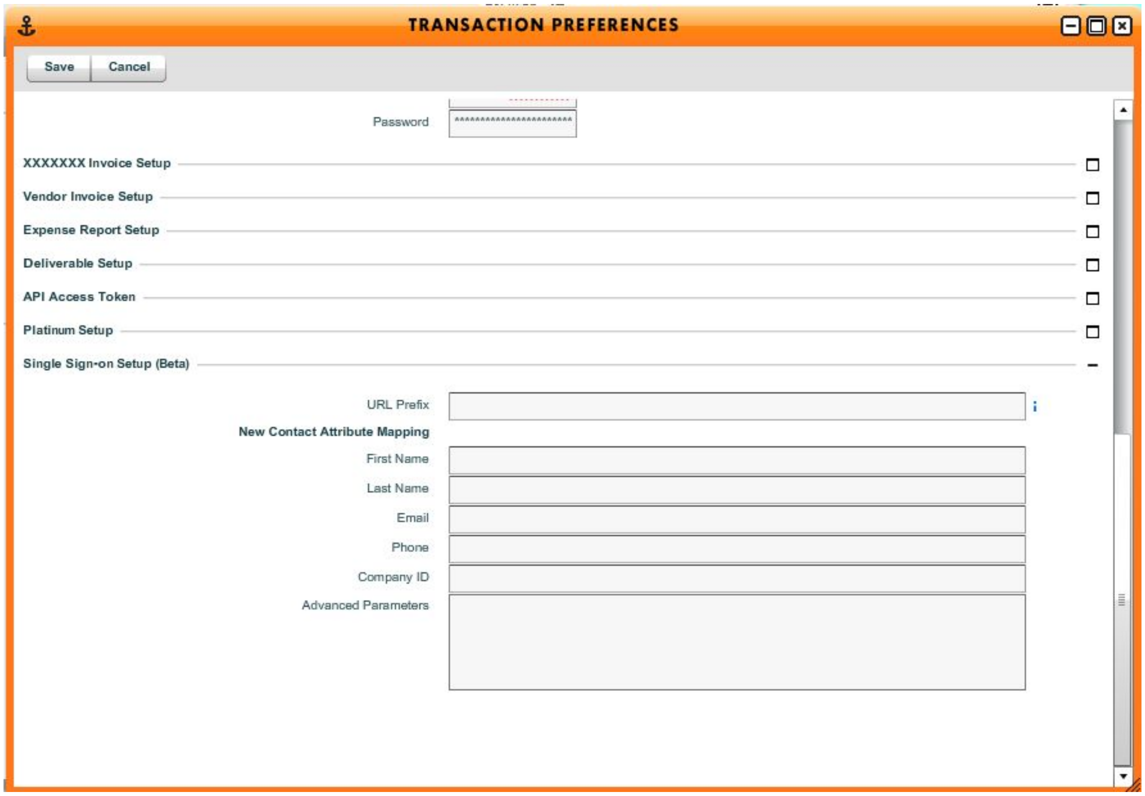
Attribute mappings
The user will need to set up attributes from their IdP to map to WMJ. UserID is automatically sent and used in WMJ as the UserID.

If a user tries to log into WMJ via the IdP and is **not** found, WMJ will attempt to create a client user given the attribute mappings

- **First Name*** - required to auto create a client login if the user was not found
- **Last Name*** - required to auto create a client login if the user was not found
- **Email** - *optional*
- **Phone** - *optional*
- **CompanyID** - *optional*. If this attribute matches a company in WMJ, the new client login will be linked to the company
- **Security Group** - *optional*. If provided and found in WMJ, the user will be assigned to that security group. If it's provided or not found, we'll use the default security group defined in the Transaction Preferences -> Client Portal -> Default Security Group setting
    - Security Group is updated everytime the user logs in.
- **Advanced Parameters** - *(not used)*

- **SAML Specific*** - This is the <PartnerIdentityProvider> name attribute specified in the saml.config file. This is how WMJ knows which PartnerIdentityProvider in the config file to use. **These must match.**

*** required for SAML to function**



Password **********************

XXXXXXX Invoice Setup □

Vendor Invoice Setup □

Expense Report Setup □

Deliverable Setup □

API Access Token □

Platinum Setup □

Single Sign-on Setup (Beta) –

URL Prefix

New Contact Attribute Mapping

First Name

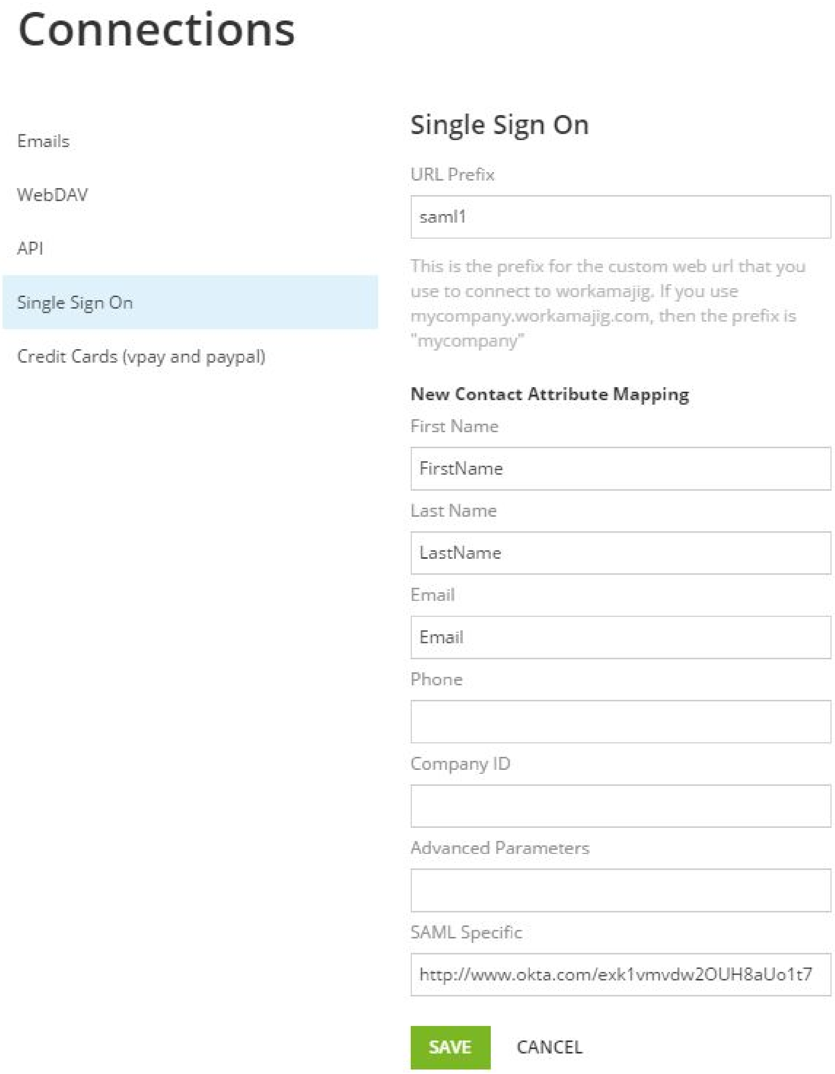
Last Name

Email

Phone

Company ID

Advanced Parameters



Connections

Single Sign On

URL Prefix: saml1

This is the prefix for the custom web url that you use to connect to workamajig. If you use mycompany.workamajig.com, then the prefix is "mycompany"

New Contact Attribute Mapping

First Name: FirstName

Last Name: LastName

Email: Email

Phone:

Company ID:

Advanced Parameters:

SAML Specific: http://www.okta.com/exk1vmvdw2OUH8aUo1t7