

Self-host Instructions for Active Directory/Single Sign-On (SSO)

To set up Comparion Self-Host with your Active Directory/SSO:

Configure saml.config

1. Open the **saml.config** file located in the installation folder (...**Application**).
2. Edit the **saml.config** parameters. This needs to be configured with the values provided by your IdP vendor.

Parameter	Description
ServiceProvider Name	The default identifier (Entity ID)
ServiceProvider Description	Identifier description (optional)
AssertionConsumerServiceUrl	The application callback URL where the response will be posted
Local Certificate FileName	To support signed requests: local certificate path
Local Certificate Password	The password you set for the local certificate
PartnerIdentityProvider Name	This value is the URL for the identity provider where your product will accept authentication requests.
SingleSignOnServiceUrl	This value defines the URL your users will be redirected to when logging in
SingleLogoutServiceUUrl	This value defines the URL your users will be redirected to when logging out
Partner Certificate Use	Use to verify that your identity provider has issued all received SAML authentication requests
Partner Certificate FileName	Certificate Path

```
<?xml version="1.0"?>
<SAMLConfiguration xmlns="urn:componentspace:SAML:2.0:configuration">
  <ServiceProvider Name="" Description="" AssertionConsumerServiceUrl="">
    <LocalCertificates>
      <Certificate FileName="" Password="" />
    </LocalCertificates>
  </ServiceProvider>
  <PartnerIdentityProviders>
    <PartnerIdentityProvider Name="" SingleLogoutServiceUrl="" SingleSignOnServiceUrl="">
      <PartnerCertificates>
        <Certificate Use="" FileName="" />
      </PartnerCertificates>
    </PartnerIdentityProvider>
  </PartnerIdentityProviders>
</SAMLConfiguration>
```

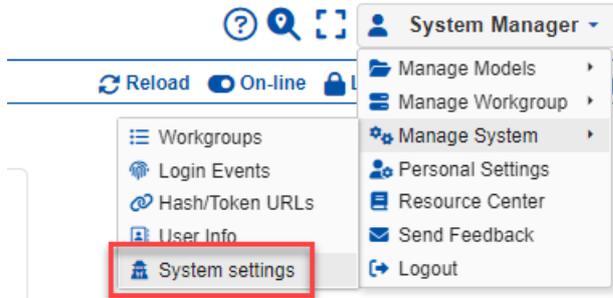
Configure appSettings.config

1. Open the **appSettings.config** file located in the installation folder (...**Application**).
2. Add the **PartnerIdP** key/value. The **PartnerIdP** key value is the same as the value you entered for **PartnerIdentityProvider Name** on **saml.config**

```
<appSettings>  
<add key="PartnerIdP" value="" />  
</appSettings>
```

Configure System Settings

1. Log in as admin
2. Go to the System Settings page (Click the username > Manage System > System settings)



or go directly to ../install/Settings.aspx

System settings

<input type="checkbox"/> FIPS mode configuration	[X]
<input checked="" type="checkbox"/> Disable Welcome (login) screen forms Auto complete	[X]
» Unsuccessful login count to lock an account: <input type="text" value="5"/>	[X]
<input type="checkbox"/> Temporary lock an account:	[X]
» Reset failed login count after (minutes): <input type="text" value="15"/>	[X]
» Automatically unlock an account after (minutes): <input type="text" value="30"/>	[X]
<input checked="" type="checkbox"/> Allow blank (empty) passwords (enabled when no password complexity)	[X]
<input type="checkbox"/> Password Complexity (Case Sensitive; At least one uppercase letter, lowercase letter, number, and special character)	[X]
» Minimum password length: <input type="text" value="4"/>	[X]
» Maximum password length: <input type="text" value="12"/>	[X]
» Minimum number of changed characters when changing password: <input type="text" value="1"/>	[X]
» Password maximum lifetime in days: <input type="text" value="2"/>	[X]
» Number of generations until a password can be reused: <input type="text" value="0"/>	[X]
<input type="checkbox"/> Ask users to set up a new password when accessing via evaluation hash link (for new users and existing users in accordance with the password setting)	[X]
<input type="checkbox"/> Enable multi-factor authentication using email address (draft)	[X]
<input type="checkbox"/> Allow to use PIN-code	[X]
<input checked="" type="checkbox"/> Check EULA when Project Organizer/Workgroup Manager logs in	[X]
<input type="checkbox"/> "Government site" mode	[X]
<input type="checkbox"/> Enable Anti-CSRF protection	[X]
<input checked="" type="checkbox"/> Use SSO (Single Sign-On) for authenticate users	[X]
<input checked="" type="checkbox"/> Allow to use only SSO for any public access (non localhost request)	[X]
» Default workgroup name when new SSO user signup: <input type="text"/>	[X]
» Default workgroup role when new SSO user signup (wm/po/eval): <input type="text"/>	[X]
<input type="checkbox"/> Administrator account should only be able to login from localhost	[X]
<input type="checkbox"/> Perform auto-logout when user idle for a session timeout (20 mins)	[X]
<input type="checkbox"/> Show draft pages (not ready for release or beta versions, HTML)	[X]

3. In the SSO setting section:
 - o Check the **Use SSO (Single Sign-On) for authenticate users**- this will show the SSO button on the login page
 - o Optional:
 - **Allow to use only SSO for any public access (non-localhost request)**- only use the SSO login option, this will hide the normal login options
 - **Default workgroup name when new SSO user signup**
 - **Default workgroup role when new SSO user signup**