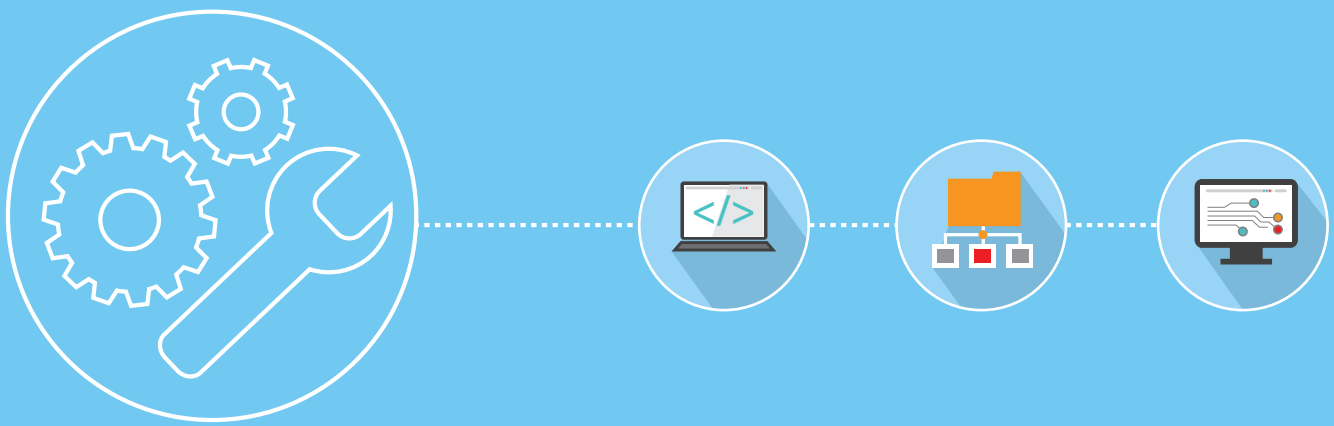
Form.com

SINGLE SIGN ON

CONFIGURATION



WEB: www.worldapp.com • www.form.com
E-MAIL: info@worldapp.com

USA: 781-849-8118
UK: +44(0) 1252 551 600
France: +33 (0)1 78 90 05 45
Australia: 1(800)-554-985
International: +44(0) 2030 020 722
Fax: 781-849-8133

WorldAPP

Introduction
This document outlines the process of **Single Sign On** functionality configuration.

Contents

www.worldapp.com | www.form.com
info@worldapp.com
USA: 781-849-8118
UK: +44(0) 1252 551 600
FR: +33 (0)1 78 90 09 45

Prerequisites

Form.com and Key Survey applications may be configured to allow Single Sign On via SAML 2 using Service Provider (SP) initiated POST binding scheme.

To use Single Sign On functionality, please be sure to setup the following prerequisites:

1. Private label (branded account) within Form.com **or** Self-Host installation;
2. Windows Server and correctly configured Active Directory.

Active Directory Federation Service (ADFS) Configuration

Note:

- Skip this section if the Windows Server has already been configured for Active Directory Federation Services.
- ADFS directory should be configured on a customer side.

To configure active directory federation service, please follow these instructions:

1. Open "Add Roles and Features" wizard in Windows Server and add "Active Directory Federation".
2. Click "Configure the federation service on this server".
3. On the "Welcome" page in the "Active Directory Federation Services Configuration" wizard, select "And" option for "Federation Server", and then click the Next button.
4. Proceed through the wizard. On the "Specify Service Properties" page, select your SSL certificate, enter a Federation Service Name, and then enter a Federation Service Display name. These names may be arbitrary.
5. Complete the "Active Directory Federation Services Configuration Wizard". Close the "Add Roles and Features Wizard".
6. If you have not created a host yet, please log the Domain Name System for the Federation Server name you specified in Step 4.

To verify the AD FS installation, do the following:

- *Open Internet Explorer on the ADFS server*
- *Browse to the URL of the Federation metadata.*
- *Turn on Compatibility View in Internet Explorer(if necessary)*
- *Verify that certificates-related warnings do not appear. If necessary, check the certificate and DNS settings.*

Trusted Relying Parties Creation

This step is required to set up the trust relationship between the ADFS and Form.com application. Please complete the following steps:

1. Open the ADFS 2.0 management console on the Federation Server.
    a. Select Trust Relationships option. Click "Relying Party Trusts" and select **Add Relying Party Trust** option.
    b. Use the following settings:
        i. Select "Enter Data about the relying party manually" Data Source option
        ii. Specify Display name. Please note, that you can use arbitrary name
        iii. Select ADFS 2.0 profile
        iv. Skip the "Configure certificate" step **and do not select** a certificate
        v. Enable SAML 2.0 WebSSO protocol support

            1. For Relying party SAML 2.0 SSO Service URL use the following: https://yourdomainname.com/Member/UserAccount/SAML2.action
        vi. Relying party trust identifiers: Add the Service Provider identifier. Arbitrary name may also be used. Please note, that this name must be sent to WorldAPP in order to configure the Form.com installation. Service provider name is the SAML2_SP_NAME configuration parameter(see below)
        vii. In "Choose Issuance Authorization Rules" select "Permit All users to access this relying party"
        viii. Review settings
        ix. On the "Finish" step tick the "Open the edit Claims Rules Dialog for this relying party trust when the wizard closes" checkbox
2. The "Edit Claims Rules Dialog" will open. Go to the "issuance Transform Rules" tab and click "Add Rule".
3. Use the setting below in the "Add Transform Claims Rule" wizard:
    a. For "Select Rule Template" select "Send LDAP Attributes as Claims"
    b. On "Configure Rule" step:
        i. Enter Claim Rule Name
        ii. For "Attribute Store" select "Active Directory"
        iii. Add the following mapping: LDAP Attribute: User Principal Name> Outgoing Claim Type: Name ID.

Configuring Private Label account for SAML SSO

The values of the following 4 parameters should be sent to the WorldAPP so that we can configure the SSO integration with your Form.com implementation:

1. **SAML2_IDP_NAME** - to obtain the value for this parameter complete the following steps:
    a. Open "AD FS 2.0" configuration console
    b. Click on "Services" > "Edit Federation Service Properties…" and copy the value specified in "Federation Service Identifier"
2. **SAML2_SP_NAME –** the value specified in step 1.b.vi in the "Configure Trusted Relying Parties" section.(that is Service provider identifier)
3. **SAML_IDP_CERT –** to provide the certificate you will need to export the certificate from the AD FS Server. Follow the steps below:
    a. Open the "AD FS 2.0" configuration console
    b. Go to "Services" > "Certificates"
    c. Select the "Token-signing" certificate, right-click on it and select "View certificate…"
    d. In the certificate window go to the "Contents tab" and press "Copy the file" button.
    e. In the certificate export wizard choose the following settings:
        i. Do not export Private Key
        ii. X.509 (.cer) with Base-64 encoding
        iii. Enter the file name and path where you would like the certificate to be saved
    f. Once exported send the file with certificate to WorldAPP.
4. **SAML2_IDP_URL -** a standard URL provided by the AD FS.

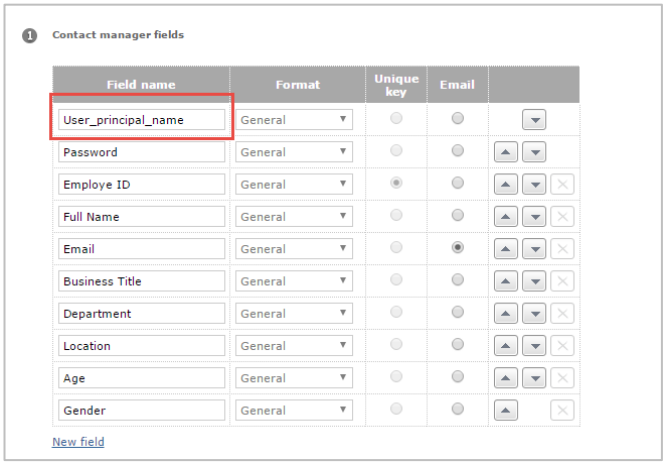
Configuring Self-Hosted account for SAML SSO

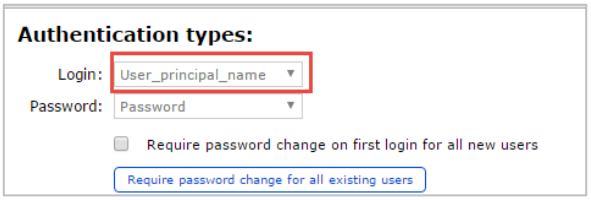
If you have a Self-Hosted instance of the application, the parameters above have to be added to the config.properties file of the application.

Configuring User Account in the Form.com application

For the Form.com application to recognize the user that logs in using the SSO, the user's login name must be identical to the value of "User-Principal-Name" property in the Active Directory, which in most cases follows the format "username@domain".

When configuring the Contact Manager and the Portal in the Form.com application, ensure that the column with the "User-Principal-Name" is present in the Contact Manager and that this column is used as a "Login" field in the Portal.





For more details on setting up the user accounts in Form.com please contact your Client Services representative.