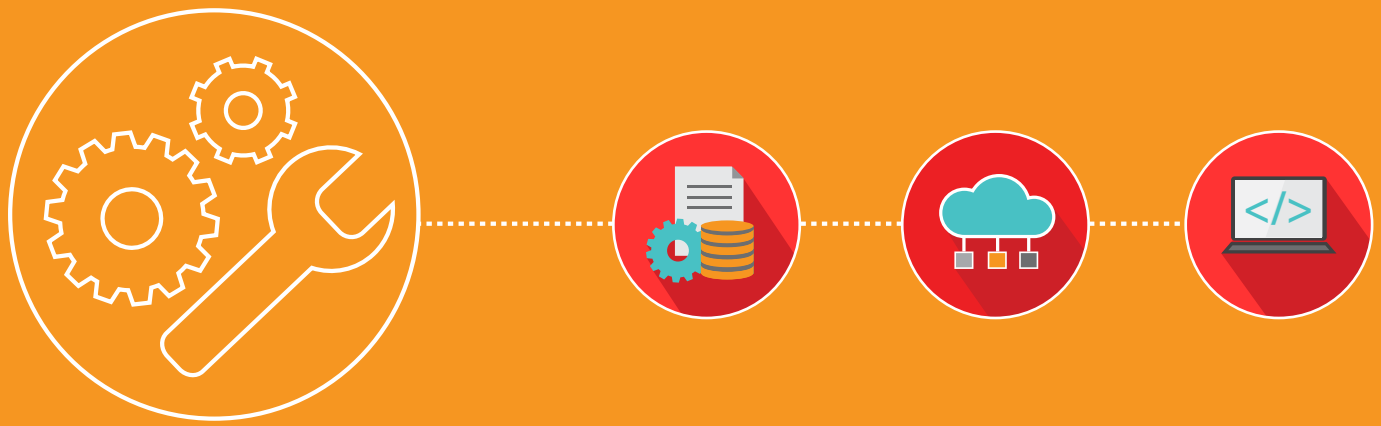
KeySurvey

SINGLE SIGN ON

CONFIGURATION



WEB: www.worldapp.com • www.keysurvey.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

Prerequisites 2
Active Directory Federation Service (ADFS) Configuration 3
Trusted Relying Parties Creation 4
Configuring Branded (Private Label) account for SAML SSO 5
Configuring Self-Hosted account for SAML SSO 5
Configuring User Account in the Key Survey application 6

Prerequisites

In order to apply Single-Sign-On functionality, following prerequisites should be configured previously:

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

Active Directory Federation Service (ADFS) Configuration

Skip this section if the Windows Server has already been configured for Active Directory Federation Services.

Note: ADFS directory should be configured on customer side.

To configure ADFS, 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", choose an option for "Federation Server", and then click Next.
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, The names entered in these fields may be arbitrary.
5. Complete the "Active Directory Federation Services Configuration Wizard". Close the "Add Riles and Features Wizard".
6. If you have not created a host, record in DNS for the federation server name you specified in Step 4 previously.

To verify the AD FS installation, do the following:

- *On the AD FS server, open Internet Explorer*
- *Browse to the URL of the Federation metadata*
- *Turn on Compatibility View in Internet Explorer(if needed)*
- *Verify that no certificates-related warnings 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 Key Survey. Please complete the following steps to set up the trust relationship on the ADFS Server:

1. Open the ADFS 2.0 management console on the Federation Server.
    a. Select Trust Relationships. Click "Relying Party Trusts" and select Add Relying Party Trust option.
    b. Use the following settings during the installation:
        - *Select Data Source option "Enter Data about the relying party manually"*
        - *Specify Display name. Arbitrary name may be used.*
        - *Choose AD FS 2.0 profile*
        - *Skip the "Configure certificate" step without selecting a certificate*
        - *Enable support for the SAML 2.0 WebSSO protocol*

            For Relying party SAML 2.0 SSO Service URL use the following: https://yourdomainname.com/Member/UserAccount/SAML2.action
        - *Relying party trust identifiers. Add the service provider identifier. Arbitrary name may be used, but this name must be sent to WorldAPP to configure the Key Survey installation, when asked for SAML2_SP_NAME configuration parameter*
        - *In "Choose Issuance Authorization Rules" select "Permit All users to access this relying party"*
        - *Review settings*
        - *On the "Finish" step check the checkbox "Open the edit Claims Rules Dialog for this relying party trust when the wizard closes"*
2. The "Edit Claims Rules Dialog" will open. Select the tab "issuance Transform Rules" and press "Add Rule".
3. Use the following settings in the "Add Transform Claims Rule" wizard:
    a. For "Select Rule Template" select "Send LDAP Attributes as Claims"
    b. On "Configure Rule" step:
        - *Enter Claim Rule Name*
        - *For "Attribute Store" select "Active Directory"*
        - *Add the following mapping: LDAP Attribute: User Principal Name> Outgoing Claim Type: Name ID.*

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

Configuring Branded (Private Label) account for SAML SSO

The values for the following 4 parameters will need to be sent to the WorldAPP team so that we can configure the SSO integration for your Key Survey 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 –** this is the value entered in step 1.b.vi in the "Configure Trusted Relying Parties" section.
3. **SAML_IDP_CERT –** to provide the certificate you will need to export the certificate from the AD FS Server using the following steps:
    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:
        - *Do not export Private Key*
        - *X.509 (.cer) with Base-64 encoding*
        - *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 –** for most configurations this will be a standard URL provided by the AD FS.

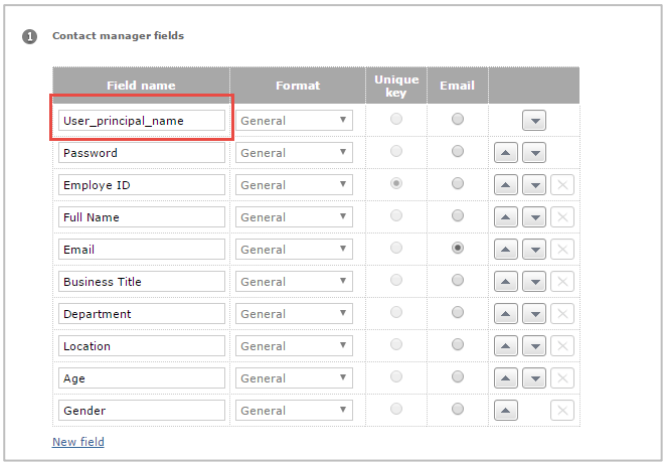
Configuring Self-Hosted account for SAML SSO

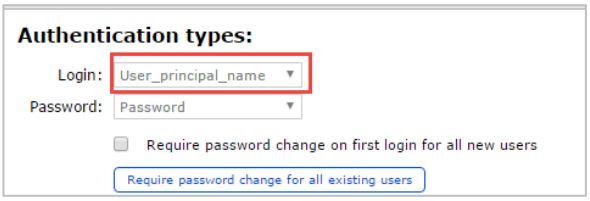
If you have a Self-Hosted instance of the application, the parameters above have to be added to the config.properties file of the application.

Configuring User Account in the Key Survey application

For the Key Survey application to recognize the user that logs in using the SSO, the user's login name must 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 Key Survey 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 Key Survey please speak with your Client Services representative.