SAML Single Sign-On Configuration for the Self-Hosted Applications and Branded Accounts

Form.com application can be configured to allow the Single Sign-On via SAML 2 using Service Provider (SP) initiated POST binding scheme. Please read the **article** for **more details**.

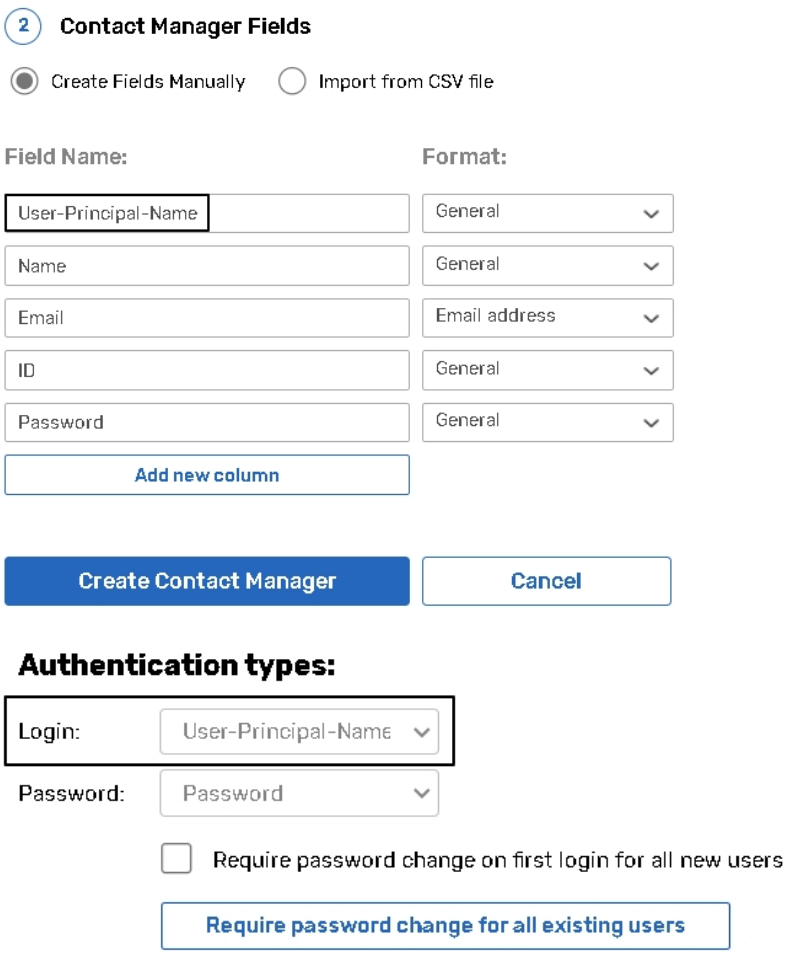
Please note that when SAML is used, the user **must exist** in the application database. So **before** the user can authenticate, a user record must be created in the application with the User Login matching the User ID returned by the Identity Provider. Depending on the type of the user, one of the following methods may be used to add users to the application:

- Adding user account via Enterprise Admin pages
- Adding a sub-account user to a Multi-Access account
- Adding a sub-account user to Multi-User account
- Adding a Portal User to access portals and mobile apps

This article describes the configuration settings in the application and on the Identity Provider side that should be made to make SAML Single Sign On possible.

Configuring the Contact Manager and the Portal

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.



Application Configuration

If your account type is **Branded/ Private Label**, the parameters below have to be provided to FORM. If you have a **Self-Hosted** instance of the application, these parameters have to be added to the **config.properties** file of the application.

EXTERNAL_AUTH.SURVEY=SAML2
SAML2_IDP_NAME.SURVEY=<IDENTITY_PROVIDER_NAME>
SAML2_SP_NAME.SURVEY=<SERVICE_PROVIDER_ IDENTIFIER>
SAML2_IDP_CERT.SURVEY=-----BEGIN CERTIFICATE-----<CERTIFICATE_PUBLIC_KEY>-----END CERTIFICATE-----
SAML2_IDP_URL.SURVEY=<AUTHENTICATION_URL>

Replace a tag with the following

Tag	Replace with
<IDENTITY_PROVIDER_NAME>	Replace it with a name of the identity provider. For example, COMPANYIDP
<SERVICE PROVIDER IDENTIFIER>	Replace the tag with the WORLDAPPSP value.
<CERTIFICATE_PUBLIC_KEY>	replace the tag with a certificate public key provided by the identity provider.
<AUTHENTICATION_URL>	specify a URL to the authentication page on the identity provider. Users will be redirected to this page when they try to access a resource that requires authentication without an active session.

<CERTIFICATE_PUBLIC_KEY>- this parameter should have multiple lines in the config file. Every line must end with **"\n\"**, except for the line where certificate ends.

Response from Identity Provider

The application is expecting one user parameter in return from the identity provider - **NameID**, which **must match** the login name of a user in the FORM system. If the system cannot find the user with such login name, **HTTP 401** error response will be sent to the user.

Single Sign-On Configuration Documentation

Here is the **PDF** document with the full description of **Single Sign-On configuration.**