Replix®

Single Sign On Configuration Guide

August 2022

Softlinx®

Web Portal Single Sign-on

Overview

The Softlinx Web Portal supports single sign-on (SSO) via the Security Assertion Markup Language (SAML). After authenticating with their Identity Provider, an SSO user will have access to the Softlinx Web Portal faxing pages. The first time a SSO user accesses the Web Portal, a corresponding replix fax user will be created. A fax number and other user attributes can be mapped from the Identity Provider to the newly created Replix user.

The Web Portal administrator will see the SSO users listed in the user list and can change attributes for these users just like they can with non SSO users.

Web Portal SSO users are created the first time an SSO user accesses the Web Portal after being authenticated by their IDP.

If the fax number attribute is mapped, then the fax number must be added to the Replix system prior to the SSO user logging into the system.

Attributes Supported

When the IdP responds with the assertion, it can optionally contain attributes (claims) about the user. The Web Portal supports the following attribute (claim) names:

- Fax
- Name
- FirstName
- LastName
- Email
- Phone
- Address1
- Address2
- Company
- Title
- DepartmentName
- ProjectCode1
- ProjectCode2

Permission claims: (Set to “YES” and at most only one permission claim should be set.)

- FaxAdmin
- Department Admin
- DepartmentPrivUser

Only one permission claim per user will be recognized. The lowest permission will take precedence. For example, if both the FaxAdmin and DepartmentAdmin claims are set for a user, the user will be granted department administration permissions. The FaxAdmin claim will be ignored.

Fax portal administrators can have a combination of individual privileges. If the user should get all of the privileges, then set the claim to "YES". Otherwise set the claim value to a comma separated list of the following options: batches, contacts, cover pages, departments, faxback, numbers, settings, users, view.

If either the DepartmentAdmin or DepartmentPrivUser claim is being used, set the value to "YES".

Note: Claim names are CASE sensitive.

Claims are configured in the Identity Provider. If the claims are present in the assertion when the user first tries to log on to the Web Portal, the attributes will be used when the corresponding Replix user is created. The attributes will NOT be used on subsequent logons. If user information changes, the administrator must use the Web Portal to change the appropriate values.

Note: FirstName and LastName will be concatenated into the Replix user’s Name field. They will only be used if the Name attribute is not in the assertion.

Configuring Single Sign-on

In order to configure single sign-on, you will need to log into your Identity Provider (IdP) and the Web Portal as an administrator. Each IdP will have different ways to set up a single sign-on instance. The sections below describe how to configure the Web Portal with the Microsoft Azure IdP and Google IdP.

When configuring both Google and Azure, you create a SAML application and configure it with URLs pointing to the Softlinx Web Portal. Then you configure the SSO settings in the Web Portal with the URLs and certificate provided by the IdP.

Microsoft Azure

1. Log into Azure as an administrator.
   https://portal.azure.com
2. Navigate to “Azure Active Directory”
3. Navigate to Manage “Enterprise Applications”
4. Create a new Application
5. Select Non-gallery application
6. Enter the display name for the new application ex: “Softlinx Fax”
7. Click the “Add” button
8. Assign the users and groups that will have access to this application.
9. Set up single sign on
10. Select SAML as the sign-on method
11. Basic SAML Configuration: (Softlinx will provide you with your organization name)
    Identifier (Entity ID):
    https://portal.rpxfax.com
    Reply URL (Assertion Consumer Service URL):
    https://portal.rpxfax.com/ACS/??? (Replace ??? with your organization name.)
    Sign on URL:
    https://portal.rpxfax.com/SSO/??? (Replace ??? with your organization name.)
12. User Attributes & Claims:
    Set a claim with the name of **Email** and the value of **user.mail**.
    Optionally set other claims as needed.
    If the id of the user is their email address, then you do not need to set the Email claim.
    You need to select “SSO ID is Email Address” in the Softlinx Portal SSO page. See step 17 below.
13. SAML Signing Certificate:
    Download the certificate (base64) to a text file. You will need to paste the contents of the certificate in a later step.
14. Make a note of the Azure AD Identifier, Login URL and Logout URL. You will use them in the following steps.
15. Log onto the Softlinx web portal as an administrator
    https://portal.rpxfax.com
16. Navigate to the settings SSO administration page.

17. Configure SSO Settings
    Enable SSO: Set to Yes

    SP Name:
    https://portal.rpxfax.com (Should match the Identifier from above.)

    IdP Name:
    The Azure AD Identifier from above.
    ex: https://sts.windows.net/c6c7e2f4-317e-4bf9-b447-e0ba24bbab4e/

    IdP URL:
    The Azure AD Identifier from above. Use the same value as IdP Name.

    Description:
    (optional)

    Single Sign-on Service URL:
    The Login URL from above.
    Ex:
    https://login.microsoftonline.com/c6c7e2f4-317e-4bf9-b447-e0ba24bbab4e/saml2

    Single Logoff Service URL:
    The Logout URL from above.
    Ex: https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0

    Certificate:
    Copy the certificate content from above.
    Example:
    -----BEGIN CERTIFICATE-----
    …
    MIIC8DCCAdigAwIBAgIQFJJHjBLNGZFN7qBfXWnFyzANBgkqhkiG9w0BAQsFA
    D0MTIwMAYDVQQD...eYXV3c7JHLEYt...
    …
    -----END CERTIFICATE-----

    IdP Assertion is using ACS/??? : set to Yes
18. Save your changes.
19. From the Azure web page, test the application.
20. To log in from the browser use: **https://portal.rpxfax.com/SSO/<org name>**

Google SSO

1. Log into Google as an administrator.
   https://admin.google.com
2. Navigate to “Apps”
3. Navigate to Manage “SAML apps”
4. Create a new Application
5. Select “SETUP MY OWN CUSTOM APP”
6. Copy the Google IdP information (SSO URL and Entity ID) to notepad for use in the following steps.
7. Download the certificate.
8. Enter the application name ex: “Softlinx Fax”
9. Configure Service Provider Details
   ACS URL:
   https://portal.rpxfax.com/ACS/??? (Replace ??? with your organization name.)
   Entity ID:
   https://portal.rpxfax.com
   Start URL:
   https://portal.rpxfax.com/SSO/??? (Replace ??? with your organization name.)
   Optionally add mappings.
   Log onto the Softlinx web portal as an administrator
   https://portal.rpxfax.com
10. Navigate to the settings SSO administration page.
11. Configure SSO Settings
    Enable SSO
    SP Name:
    https://portal.rpxfax.com (should match the Entity ID from above)
    IdP Name:
    The Entity ID from above.
    ex: https://accounts.google.com/o/saml2?idpid=C046f0i93
    IdP URL:
    Same as IdP name.
    Description:
    (optional)
    Single Sign-on Service URL:
    The SSO URL from above.
    Ex: https://accounts.google.com/o/saml2/idp?idpid=C046f0i93

12. **Certificate:**
    Copy the certificate content from above.
    Ex: -----BEGIN CERTIFICATE-----
    MIIC8DCCAdigAwIBAgIQFJJHjBLNGZFN7qBfXWnFyzANBgkqhkiG9w0BAQsFADA
    ...eYXV3c7JHLEYtxTj4L4v
    -----END CERTIFICATE-----
13. Save your changes.
14. From the Google web page, test the application.
15. To log in from the browser use: **https://portal.rpxfax.com/SSO/<org name>**