Softlinx

Single Sign-on

Windows Desktop Client

8-24-2022

Contents

Single Sign-on For Windows Desktop Client

Overview

The Windows Desktop Client will communicate with Microsoft Azure or Google Identity Providers in order to support single sign-on for users. The goal of single sign-on is to allow the end user to enter their credentials into the appropriate Identify Provider's portal and then gain access to the Windows Desktop Client.

When SSO is configured properly, the end user will be shown a "Login Microsoft" or "Login Google" button on the Windows Desktop Client's logon dialog. They will not enter credentials directly into the Windows Desktop Client. After pressing the Login button, they will be prompted with the Identity Provider's logon page. If Google is the Identity Provider, a browser window will open. If Microsoft is the Identity Provider, a Microsoft logon window will appear.

After entering the correct credentials, the Windows Desktop Client will allow the user access to the application to send and query faxes. Similar to the SSO support in the Web Portal, a corresponding Replix user will be created in order to allow the faxing functionality.

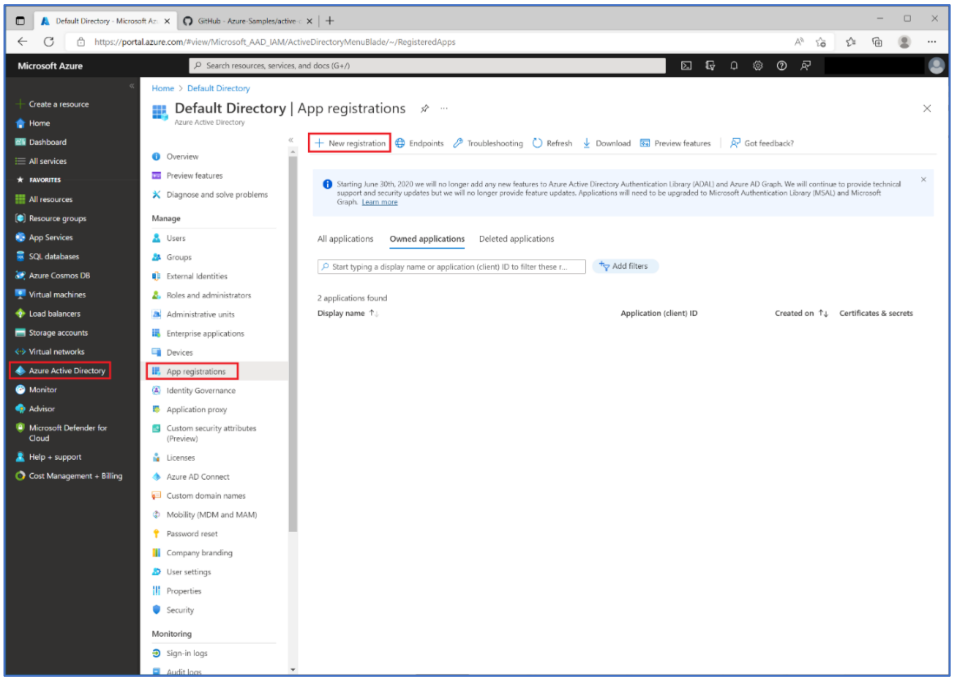
Setup Overview

1. The customer registers an application in their Azure or Google account.
2. The unique identifiers for this app then need to be added to the Softlinx cloud for the organization via the web portal (Administration -> Settings -> SSO). This will allow the mapping of the unique Identity Provider application ID to a Softlinx Organization.
3. During installation of the Windows Desktop client, the user can select the appropriate Identity Provider and enter the same IDs. This can optionally be done after installation.

Creating Microsoft Azure Application

Open a browser and go to: http://portal.azure.com

Navigate to Azure Active Directory -> App Registration. Select “New Registration”.



Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

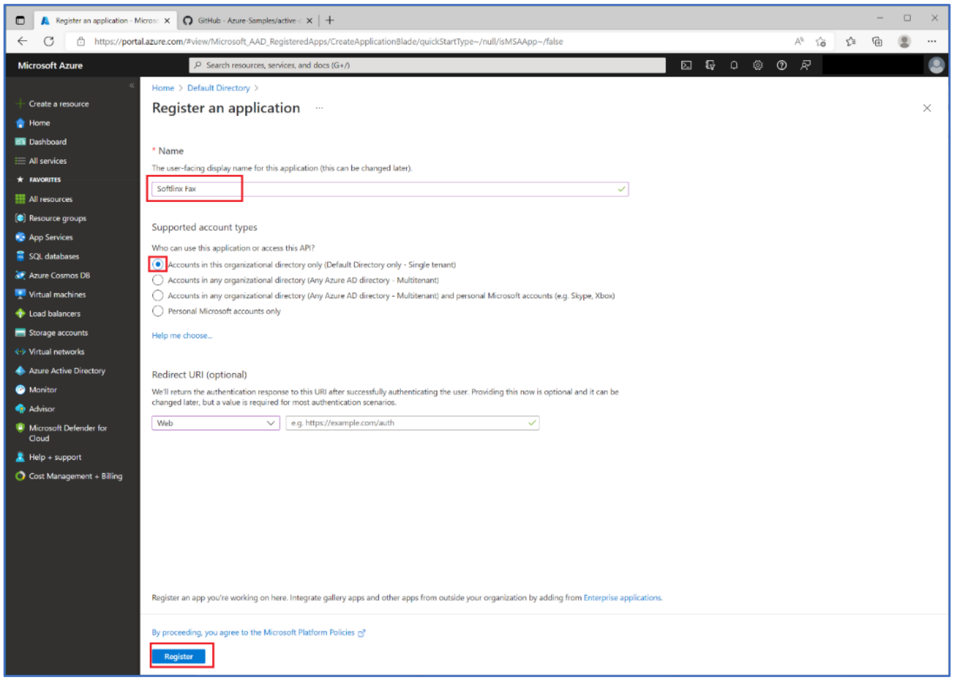
All applications | Owned applications | Deleted applications

Start typing a display name or application (client) ID to filter these r... | Add filters

2 applications found

Display name ↑↓	Application (client) ID	Created on ↑↓	Certificates & secrets

Enter the name of the application, such as “Softlinx Fax”. Then select who can use this application. You should select “Accounts in this organization directory only…”. Select “Register”.


Register an application - Microsc
GitHub - Azure-Samples/active-
https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/CreateApplicationBlade/quickStartType~/null/isMSAApp~/false
Microsoft Azure
Search resources, services, and docs (G+/)
[redacted]
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Microsoft Defender for Cloud
Help + support
Cost Management + Billing
Home > Default Directory >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Softlinx Fax

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Default Directory only - Single tenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

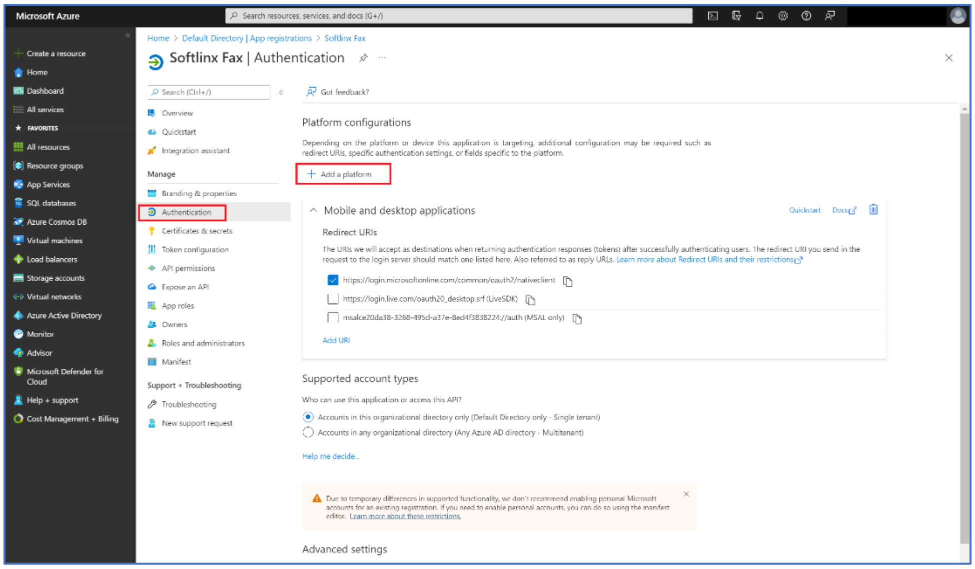
Web | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

Register

Now select “Add a Platform”.



Softlinx Fax | Authentication

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

Mobile and desktop applications

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

- ☑ https://login.microsoftonline.com/common/oauth2/nativeclient
- ☐ https://login.live.com/oauth20_desktop.srf (LiveSDK)
- ☐ msalce20da38-3268-495d-a37e-8ed4f3838224://auth (MSAL only)

Supported account types

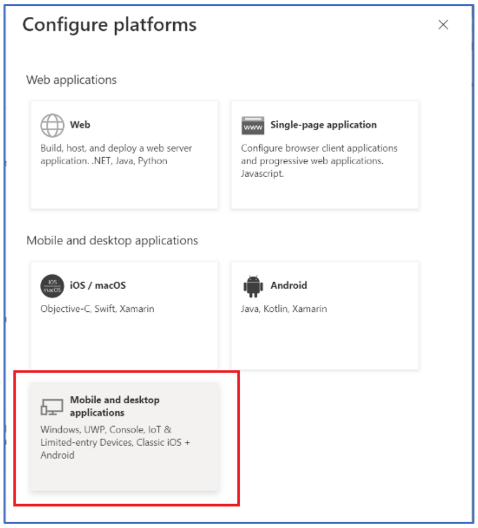
Who can use this application or access this API?

- ● Accounts in this organizational directory only (Default Directory only - Single tenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.

Advanced settings

Select “Mobile and desktop applications”.



Configure platforms

Web applications

Web
Build, host, and deploy a web server application. .NET, Java, Python

Single-page application
Configure browser client applications and progressive web applications. Javascript.

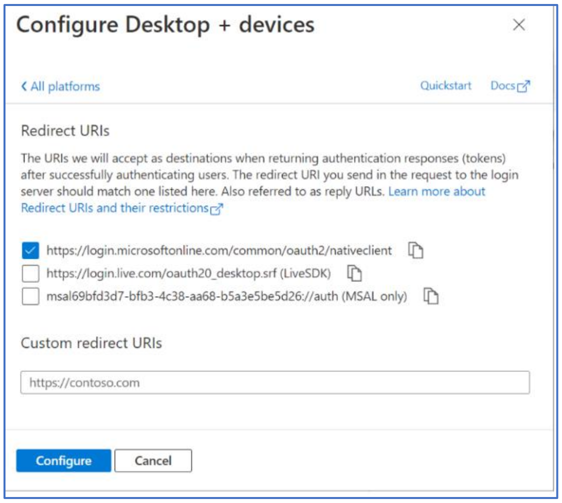
Mobile and desktop applications

iOS / macOS
Objective-C, Swift, Xamarin

Android
Java, Kotlin, Xamarin

Mobile and desktop applications
Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android

Make sure the oauth2 URL is selected. Then press "Configure".



Configure Desktop + devices

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

☑ https://login.microsoftonline.com/common/oauth2/nativeclient

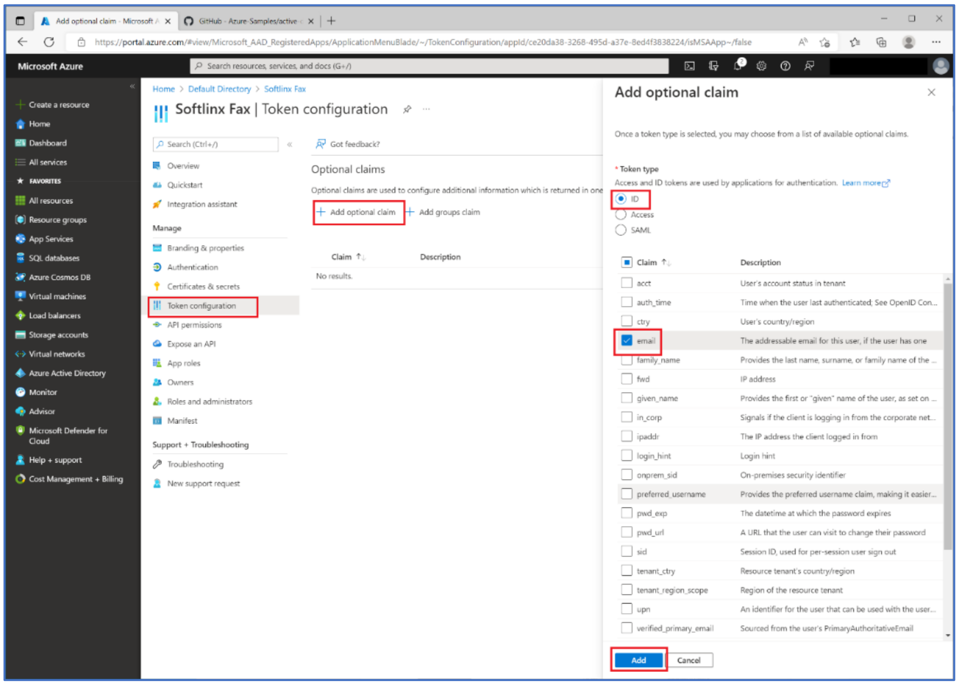
□ https://login.live.com/oauth20_desktop.srf (LiveSDK)

□ msal69bfd3d7-bfb3-4c38-aa68-b5a3e5be5d26://auth (MSAL only)

Custom redirect URIs

https://contoso.com

Navigate to "Token Configuration" and then select "Add optional claim". Select "ID" as the token type and select the "email" claim. Then press "Add".



https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/TokenConfiguration/appId/ce20da38-3268-495d-a37e-8ed4f3838224/isMSAApp~/false

[redacted]

Softlinx Fax | Token configuration

Optional claims

Optional claims are used to configure additional information which is returned in one

Claim	Description
No results.	

Add optional claim

Once a token type is selected, you may choose from a list of available optional claims.

* Token type

Access and ID tokens are used by applications for authentication. Learn more

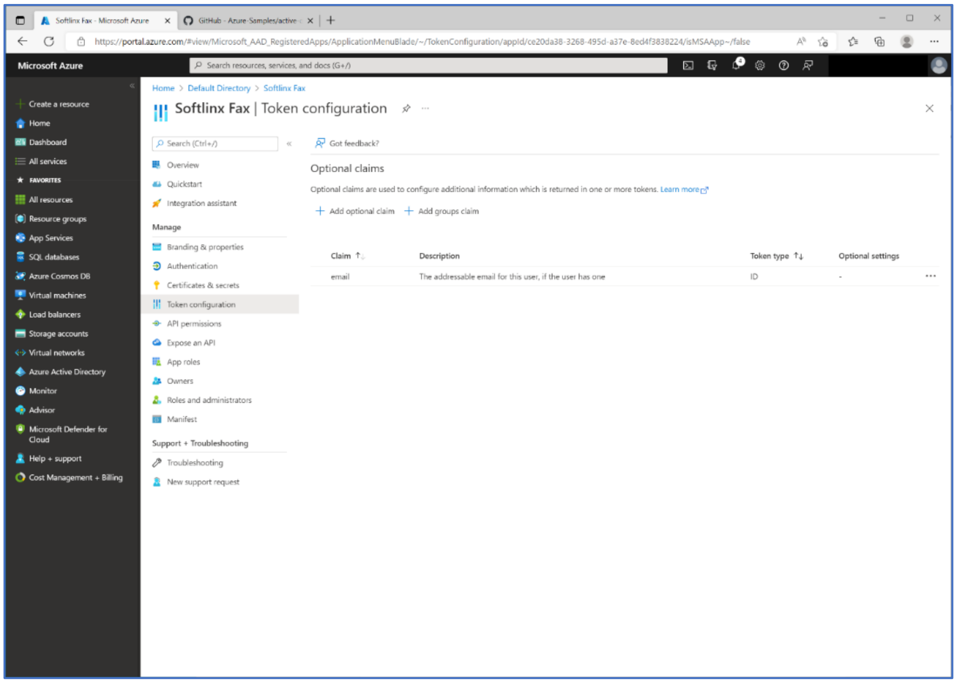
● ID

○ Access

○ SAML

	Claim	Description
□	acct	User's account status in tenant
□	auth_time	Time when the user last authenticated; See OpenID Con...
□	ctry	User's country/region
☑	email	The addressable email for this user, if the user has one
□	family_name	Provides the last name, surname, or family name of the ...
□	fwd	IP address
□	given_name	Provides the first or "given" name of the user, as set on ...
□	in_corp	Signals if the client is logging in from the corporate net...
□	ipaddr	The IP address the client logged in from
□	login_hint	Login hint
□	onprem_sid	On-premises security identifier
□	preferred_username	Provides the preferred username claim, making it easier...
□	pwd_exp	The datetime at which the password expires
□	pwd_url	A URL that the user can visit to change their password
□	sid	Session ID, used for per-session user sign out
□	tenant_ctry	Resource tenant's country/region
□	tenant_region_scope	Region of the resource tenant
□	upn	An identifier for the user that can be used with the user...
□	verified_primary_email	Sourced from the user's PrimaryAuthoritativeEmail

This is what you should see after the claim is added.



[redacted]

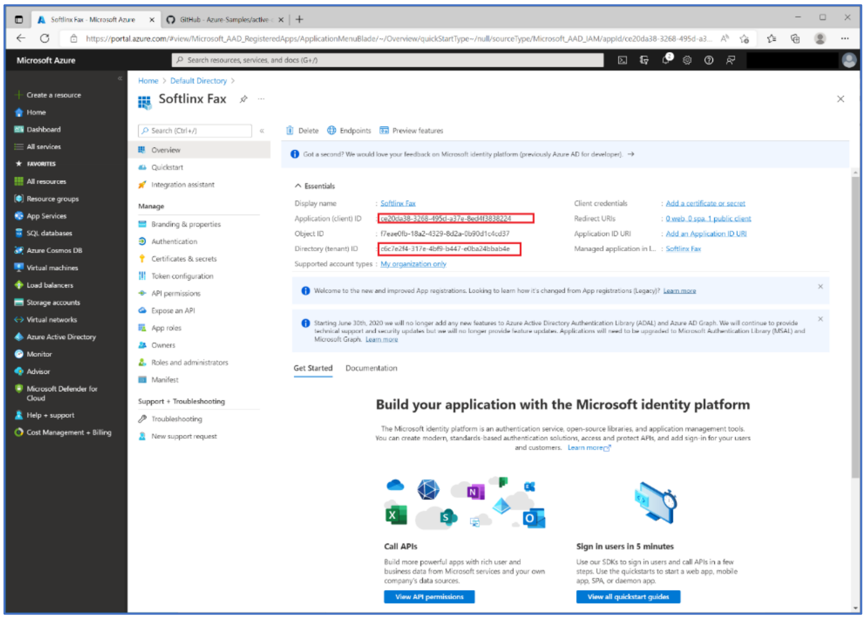
Softlinx Fax | Token configuration

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim	Description	Token type	Optional settings
email	The addressable email for this user, if the user has one	ID	-

Now select “Overview”. You will need the Application ID and Directory ID in the following steps when configuring the Softlinx portal and installing the Windows Desktop client.



[redacted]

Softlinx Fax

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : Softlinx Fax
Application (client) ID : ce20da38-3268-495d-a37e-8ed4f3838224
Object ID : f7eae0fb-18a2-4329-8d2a-0b90d1c4cd37
Directory (tenant) ID : c6c7e2f4-317e-4bf9-b447-e0ba24bbab4e
Supported account types : My organization only
Client credentials : Add a certificate or secret
Redirect URIs : 0 web, 0 spa, 1 public client
Application ID URI : Add an Application ID URI
Managed application in l... : Softlinx Fax

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Sign in users in 5 minutes

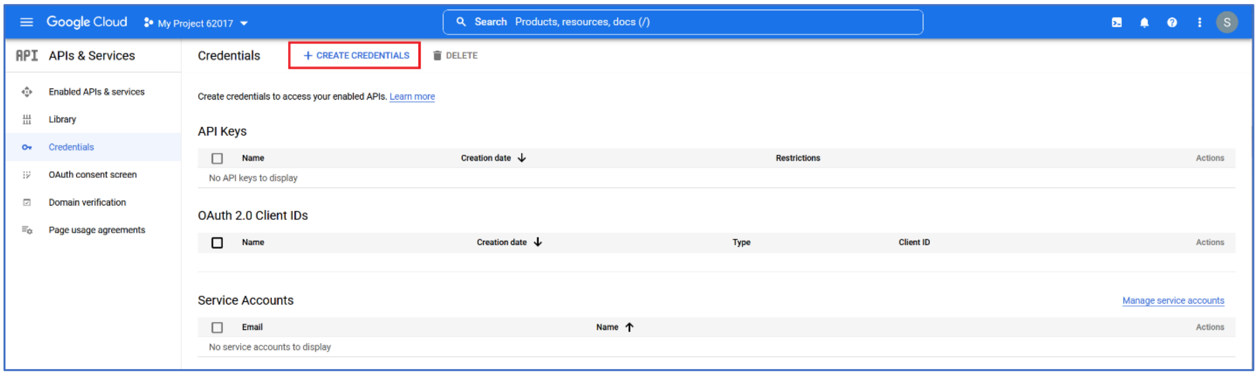
Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app.

Go to the Configuring SSO on Softlinx Portal (page 10) section.

Configuring Google

Open a browser and go to: https://console.cloud.google.com

Navigate to: API & Services -> Credentials ->Create Credentials



Create credentials to access your enabled APIs. Learn more

API Keys

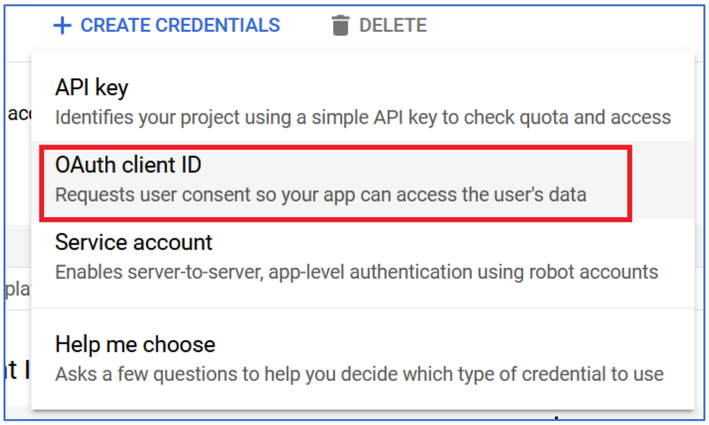
□	Name	Creation date ↓	Restrictions	Actions
No API keys to display				

OAuth 2.0 Client IDs

□	Name	Creation date ↓	Type	Client ID	Actions

Service Accounts

□	Email	Name ↑	Actions
No service accounts to display			

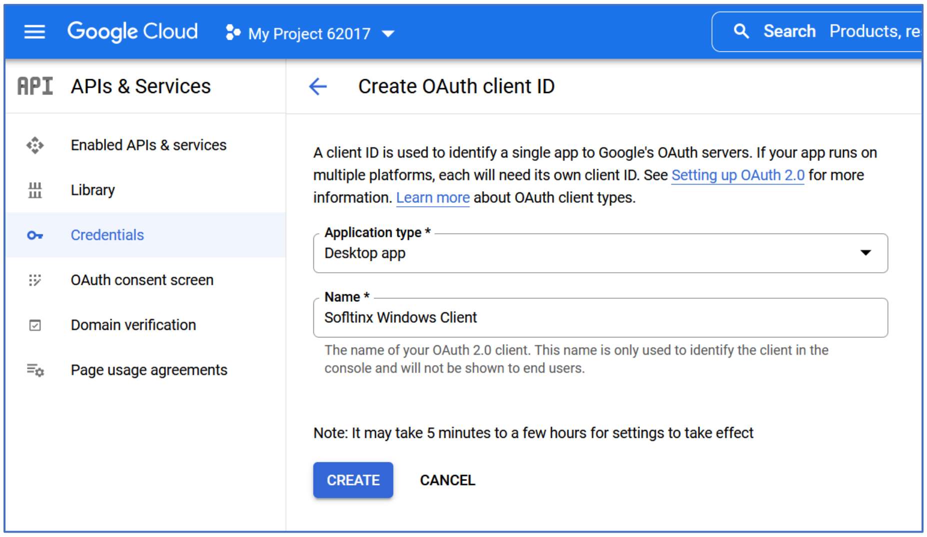


API key
Identifies your project using a simple API key to check quota and access

OAuth client ID
Requests user consent so your app can access the user's data

Service account
Enables server-to-server, app-level authentication using robot accounts

Help me choose
Asks a few questions to help you decide which type of credential to use



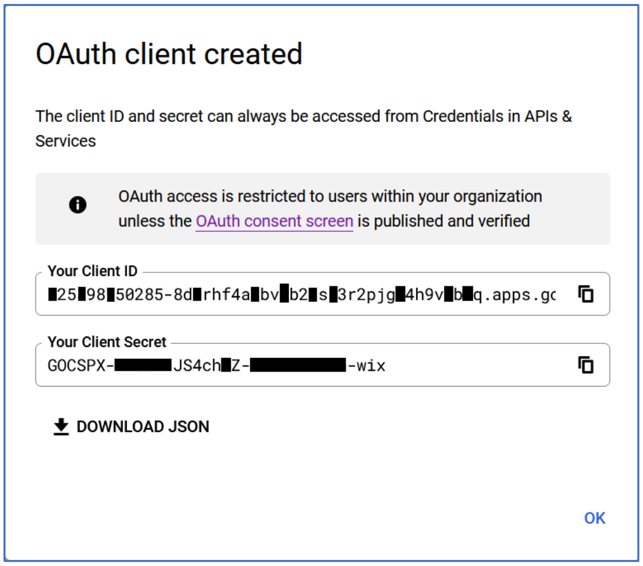
A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See Setting up OAuth 2.0 for more information. Learn more about OAuth client types.

Application type *
Desktop app

Name *
Softlinx Windows Client

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

Note: It may take 5 minutes to a few hours for settings to take effect



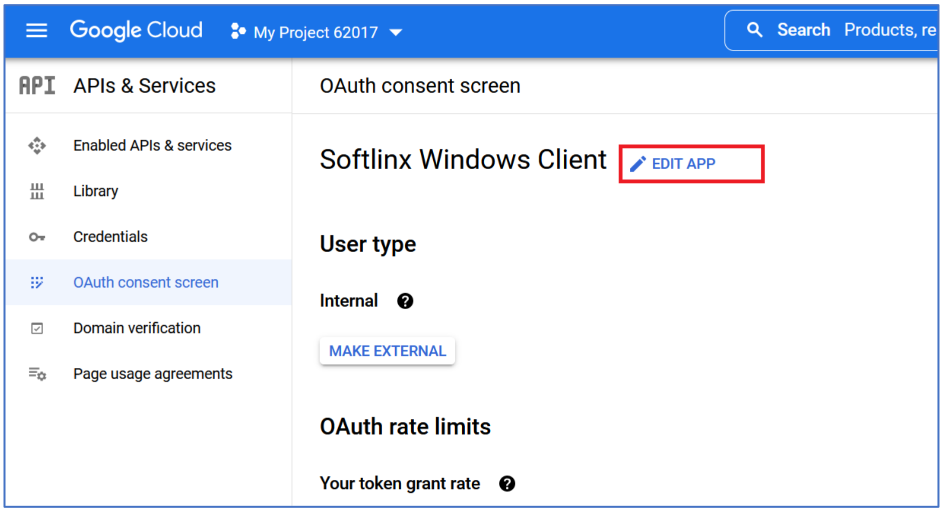
OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

OAuth access is restricted to users within your organization unless the OAuth consent screen is published and verified

Your Client ID
[redacted]25[redacted]98[redacted]50285-8d[redacted]rhf4a[redacted]bv[redacted]b2[redacted]s[redacted]3r2pjg[redacted]4h9v[redacted]b[redacted]q.apps.gc

Your Client Secret
GOCSPX-[redacted]JS4ch[redacted]Z-[redacted]-wix



Softlinx Windows Client

User type

Internal

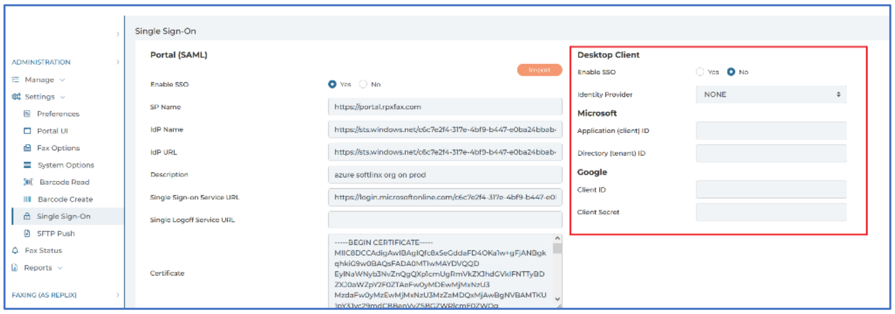
OAuth rate limits

Your token grant rate

Configuring SSO on Softlinx Portal

Log on as an administrator and navigate to Administration -> Settings -> SSO.

Select the Identity Provider and set the corresponding IDs. These IDs are from registering the Azure App or Google Oauth Client. Select “Save”.



Single Sign-On

Portal (SAML)

Enable SSO ● Yes ○ No

SP Name: https://portal.rpxfax.com

IdP Name: https://sts.windows.net/c6c7e2f4-317e-4bf9-b447-e0ba24bbab

IdP URL: https://sts.windows.net/c6c7e2f4-317e-4bf9-b447-e0ba24bbab

Description: azure softlinx org on prod

Single Sign-on Service URL: https://login.microsoftonline.com/c6c7e2f4-317e-4bf9-b447-e0l

Single Logoff Service URL:

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQfc8xSeGddaFD4OKa1w+gFjANBgk
qhkiG9w0BAQsFADA0MTIwMAYDVQQD
EyINaWNyb3NvZnQgQXplcmUgRmVkZXJhdGVkIFNTTyBD
ZXJ0aWZpY2F0ZTAeFw0yMDEwMjMxNzU3
MzdaFw0yMzEwMjMxNzU3MzZaMDQxMjAwBgNVBAMTKU
IpY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQg
```

Desktop Client

Enable SSO ○ Yes ● No

Identity Provider: NONE

Microsoft

Application (client) ID:

Directory (tenant) ID:

Google

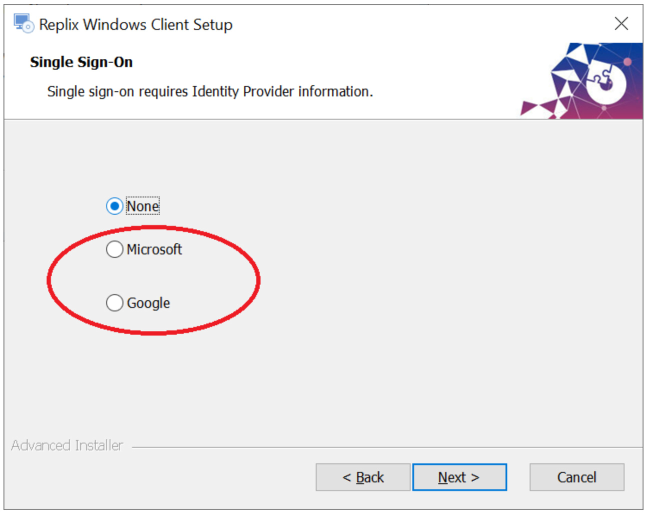
Client ID:

Client Secret:

Now you can install the Windows Desktop client.

Configuring Windows Desktop Client for SSO

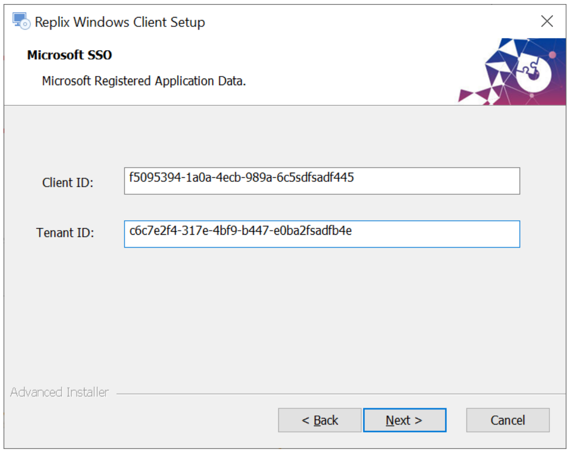
When installing the Windows Desktop Client, select the appropriate Identity Provider and then enter the correct IDs:


Replix Windows Client Setup

Single Sign-On

Single sign-on requires Identity Provider information.

● None
○ Microsoft
○ Google


Replix Windows Client Setup

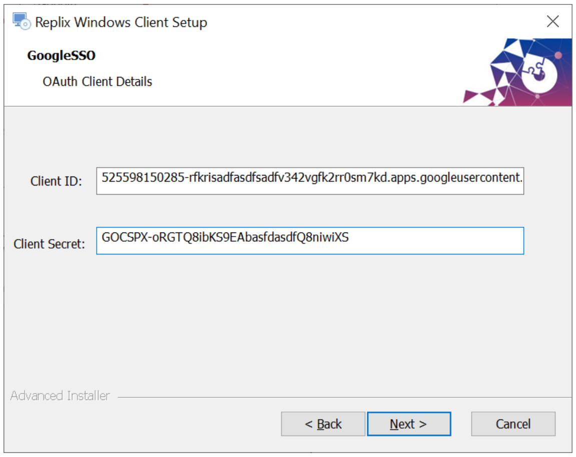
Microsoft SSO

Microsoft Registered Application Data.

Client ID: f5095394-1a0a-4ecb-989a-6c5sdfsadf445

Tenant ID: c6c7e2f4-317e-4bf9-b447-e0ba2fsadfb4e

or


Replix Windows Client Setup

GoogleSSO

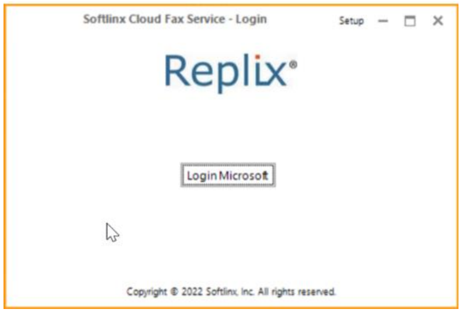
OAuth Client Details

Client ID: 525598150285-rfkrisadfasdfsadfv342vgfk2rr0sm7kd.apps.googleusercontent.

Client Secret: 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XS

After the installation is complete, start the Windows Desktop client by double clicking on the icon or printing a document the Replix Fax printer.

You should see a logon page with a logon button (either for Microsoft or Google). The example below is for a Microsoft Identity Provider setup.

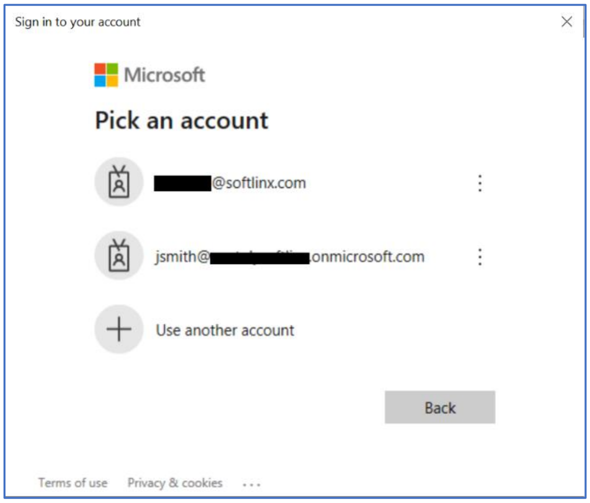

Softlinx Cloud Fax Service - Login

Copyright © 2022 Softlinx, Inc. All rights reserved.

Logging in as SSO user to Windows Desktop Client

Select the “Login Microsoft” button or “Login Google” button from the Windows Desktop client UI. If Microsoft is the Identity Provider, then the Microsoft login page will appear (see below). If Google is the Identity Provider, a browser window will appear and you will be directed to the Google SSO logon page.

Select your Microsoft account.



Sign in to your account

Microsoft

Pick an account

[redacted]@softlinx.com

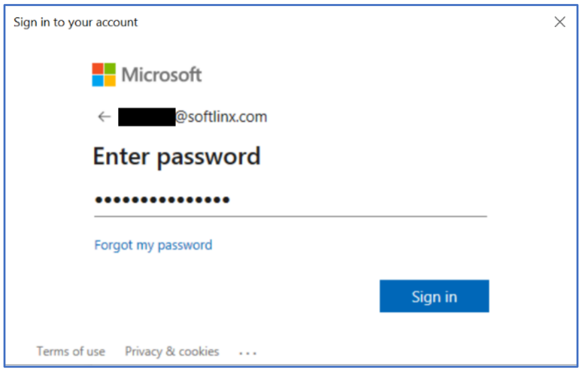
jsmith@[redacted]onmicrosoft.com

Use another account

Back

Terms of use   Privacy & cookies   ...

Enter your password.



Sign in to your account

Microsoft

← [redacted]@softlinx.com

Enter password

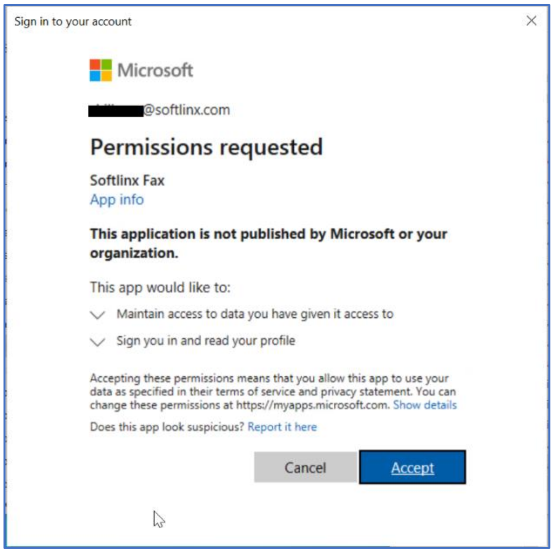
•••••••••••••••

Forgot my password

Sign in

Terms of use   Privacy & cookies   ...

Allow access.


Sign in to your account

Microsoft

[redacted]@softlinx.com

Permissions requested

Softlinx Fax

App info

This application is not published by Microsoft or your organization.

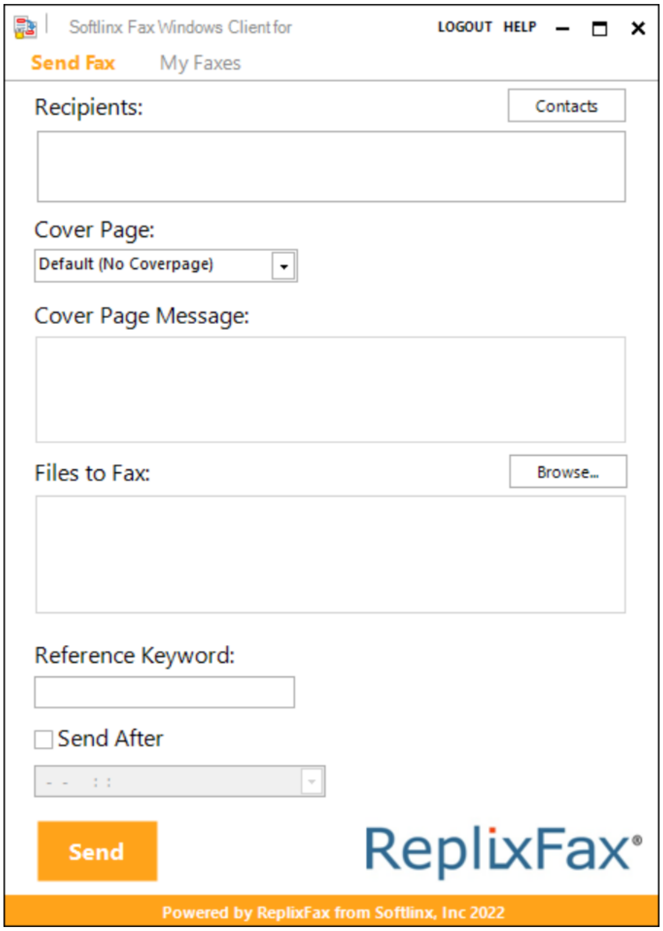
This app would like to:

- Maintain access to data you have given it access to
- Sign you in and read your profile

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

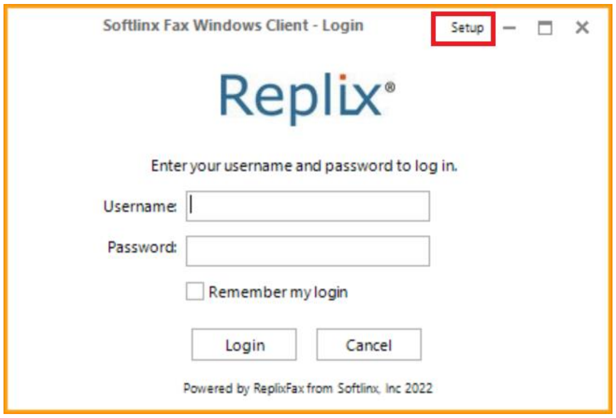
Does this app look suspicious? Report it here

After a successful logon, the main Windows Desktop Application window will appear. The change password button will NOT be visible.


Softlinx Fax Windows Client for

Cover Page: Default (No Coverpage)

If the Windows Desktop Client is already installed and you did not configure SSO, then you can still configure SSO. You must start the Windows Desktop client as an administrator. From the logon dialog, select the settings menu.



Enter your username and password to log in.

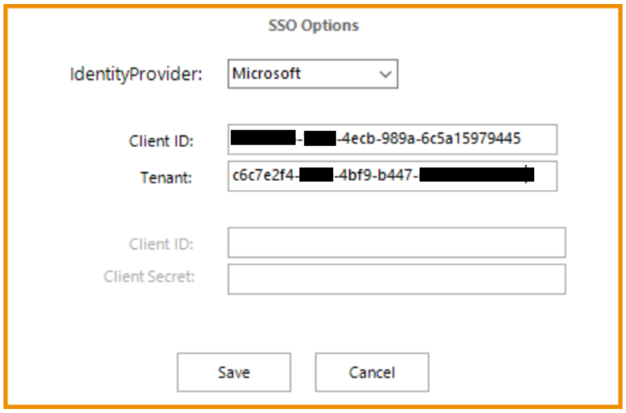
Username:

Password:

☐ Remember my login

Powered by ReplixFax from Softlinx, Inc 2022

Select the appropriate Identity Provider and corresponding IDs.



IdentityProvider: Microsoft

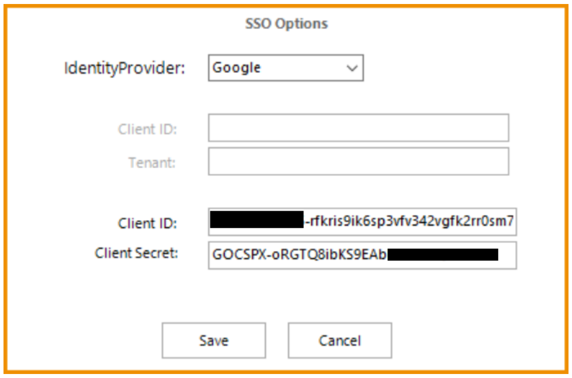
Client ID: [redacted]-[redacted]-4ecb-989a-6c5a15979445

Tenant: c6c7e2f4-[redacted]-4bf9-b447-[redacted]

Client ID:

Client Secret:

Figure 1Microsoft Identity Provider



IdentityProvider: Google

Client ID:

Tenant:

Client ID: [redacted]-rfkris9ik6sp3vfv342vgfk2rr0sm7

Client Secret: GOCSPX-oRGTQ8ibKS9EAb[redacted]

Figure 2Google Identity Provider

Save your changes.