Single Sign-on with Azure Active Directory

Version 19.05.28

March 2019

Table of Contents

Overview and Requirements for single sign-on 4

1. What is Single Sign-on (SSO)? 4

2. Who is eligible for SSO? 4

3. What are the requirements for SSO? 4

4. What is the process if an SSO enabled company adds new users? 4

5. Where can stratafax customers use SSO? 4

6. What notification will stratafax send out after SSO is enabled? 4

7. In the case that SSO server failed or customers are not able to sign in with SSO, what should they do? 4

8. How can stratafax customers set up their SSO settings? 5

Configure single sign-on to stratafax application in Azure Active Directory 6

SAML-based single sign-on 7

Enter basic SAML configuration 7

Review certificate expiration data, status, and email notification 8

Set up stratafax application to authenticate through Azure AD 8

Assign users and groups to your stratafax SAML application 9

Test the SAML application 9

stratafax user creation 9

Manual creation of users 9

Synchronize users 10

stratafax Web Client and Printer Driver authentication with SSO 10

1. stratafax Web Client 10

2. stratafax Printer Driver 10

stratafax IP Printer Download 10

stratafax IP Printer Prerequisites 10

stratafax IP Printer Installation Instructions 10

Using the stratafax IP Printer to Quickly Distribute Documents 13

Overview and Requirements for single sign-on

1. What is Single Sign-on (SSO)?

Single Sign-on allows employees in a company to access all the company applications with one set of credentials. Depending on the company, the credentials can include email, phone number or username, along with the password. The company routes all logins through an IDP (Identity Provider) with which the company has a purchased license. The IDP usually hosts a login page for the employees to enter their company credentials before entering any application. Single Sign-on provides better security with the central authentication point, limiting the possibility of phishing.

QUICK TIP: To ensure there is no conflict with Single Sign-on for your account, each user contact email address must be unique when creating user extensions or call queue extensions.

2. Who is eligible for SSO?

stratafax Secure subscription is eligible for SSO. Please contact your Account Manager if you have questions regarding your subscription type.

3. What are the requirements for SSO?

An IDP (Identity provider) which supports **SAML 2.0** is required. Most IDPs in the industry support **SAML2.0**, but it should still be confirmed before the SSO implementation.

4. What is the process if an SSO enabled company adds new users?

The new user will receive an activation email for the account to setup their PIN & security questions. The email will include instructions for them to sign in with SSO.

5. Where can stratafax customers use SSO?

SSO works with your stratafax online account and the stratafax web application.

6. What notification will stratafax send out after SSO is enabled?

stratafax will not send any notifications. It will be the customer who will need to send out the notification and let their employees know about the change after SSO is enabled.

7. In the case that SSO server failed or customers are not able to sign in with SSO, what should they do?

Customers can reach out to stratafax support. You may need to check your Azure AD authentication to make sure it is reachable and redirecting to stratafax before reaching out to stratafax support.

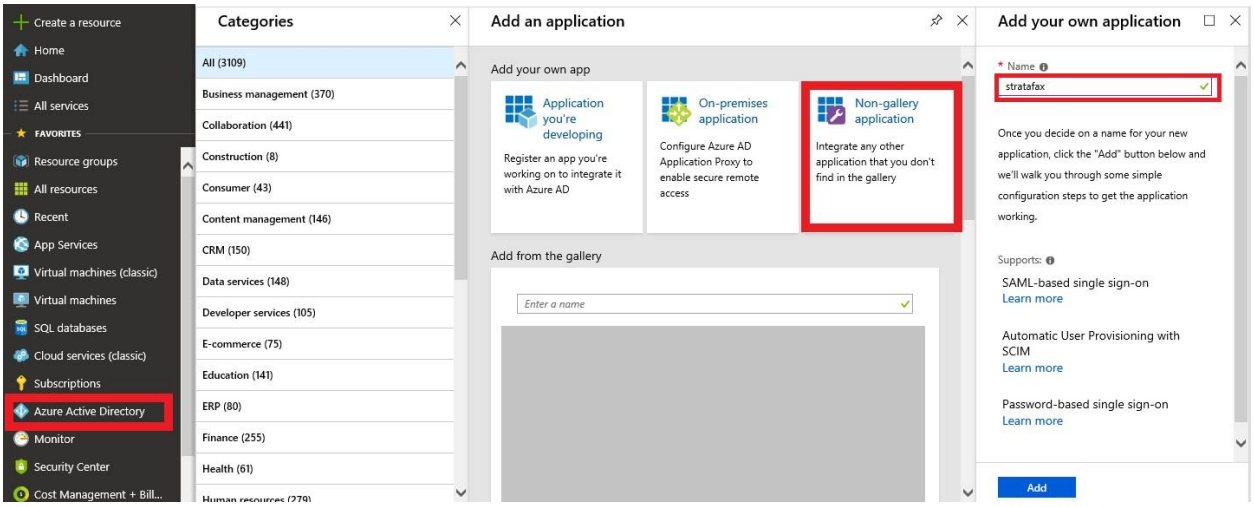
8. How can stratafax customers set up their SSO settings?

You will need to work with stratafax to setup SSO. Here are the requirements for setting up Windows Azure SSO using SALM authentication.

1. Customer must already have an Azure AD subscription and have users synchronized to Azure Active Directory.
2. Configure single sign-on in Azure Active Directory (see instructions below)
3. Provide stratafax a copy of the Base64 certification from the Application settings, under the Single Sign-on configuration.
4. Users have to be created manually, imported into stratafax or synchronized using Secure LDAP and configured for External authentication.
5.

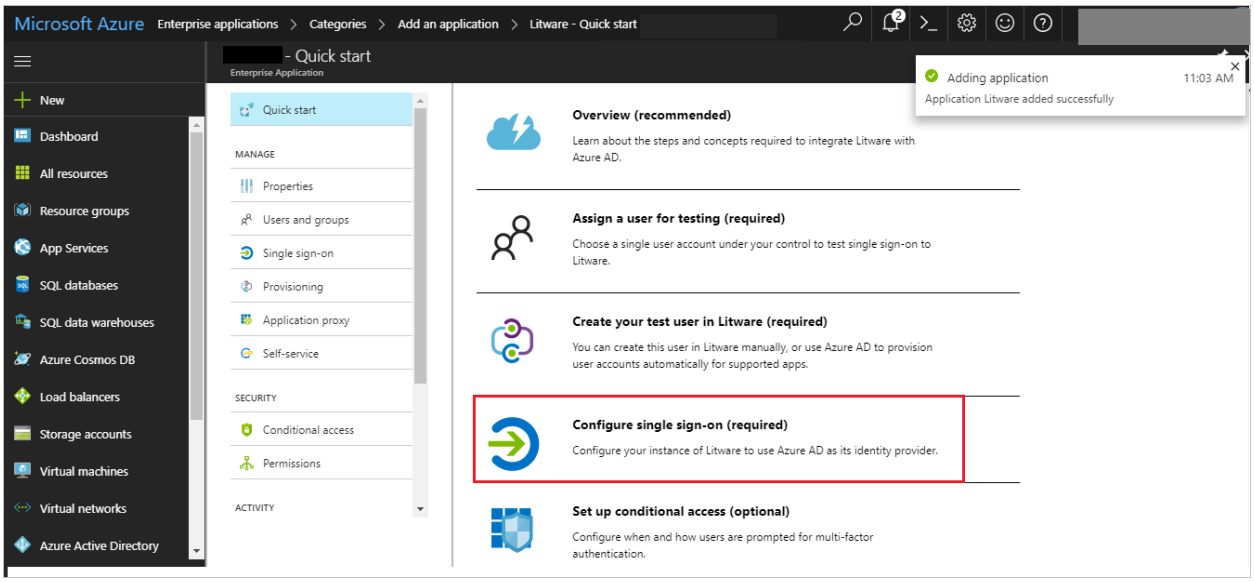
Configure single sign-on to stratafax application in Azure Active Directory

To connect an application using an app integration template, sign in to the Azure portal using your Azure Active Directory administrator account. Browse to the **Active Directory > Enterprise Applications > New application > Non-gallery application** section, select **Add**, and then **Add an application from the gallery**.

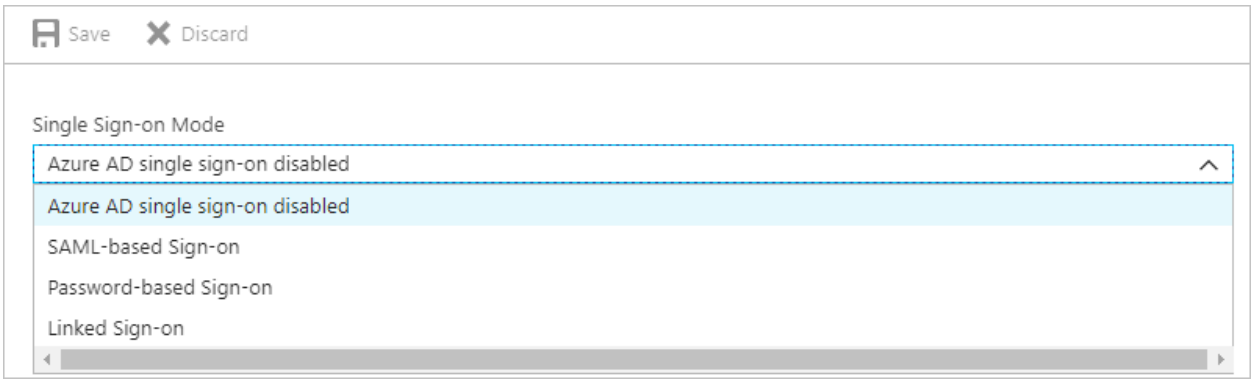


Reference this link for additional details: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-single-sign-on-non-gallery-applications

After entering a Name for your application (stratafax), you can configure the single sign-on options and behavior.



Adding an application this way provides a similar experience to the one available for pre-integrated applications. To start, select **Configure Single Sign-On** or click on **Single sign-on** from the application's left-hand navigation menu. The next screen presents the options for configuring single sign-on. The options are described in the next sections of this article.

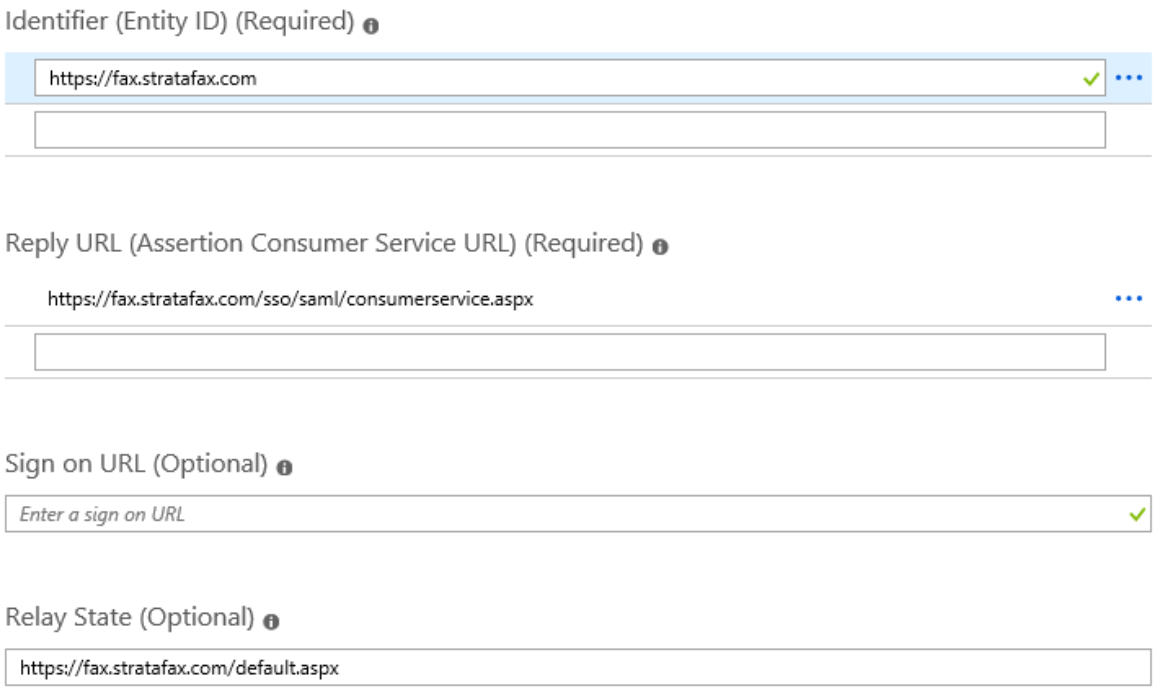


SAML-based single sign-on

Select this option to configure SAML-based authentication for the application. This requires that the application support SAML 2.0. You should collect information on how to use the SAML capabilities of the application before continuing. Complete the following sections to configure single sign-on between the application and Azure AD.

Enter basic SAML configuration

To set up Azure AD, enter the basic SAML configuration. You can manually enter the values or upload a metadata file to extract the value of the fields.



Identifier - should uniquely identify the application for which single sign-on is being configured. You can find this value as the Issuer element in the AuthRequest (SAML request) sent by the application. This

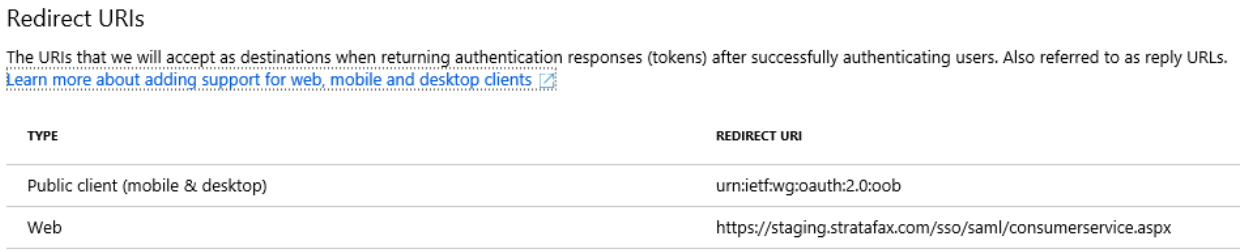
value also appears as the **Entity ID** in any SAML metadata provided by the application. Check the application's SAML documentation for details on what its Entity ID or Audience value is.

Reply URL - The reply URL is where the application expects to receive the SAML token. This is also referred to as the Assertion Consumer Service (ACS) URL. Check the application's SAML documentation for details on what its SAML token reply URL or ACS URL is.

Redirect URI – The redirect_uri of your app, where authentication responses can be sent and received by your app. It must exactly match one of the redirect_uris you registered in the portal, except it must be url encoded. For native & mobile apps, you should use the default value of urn:ietf:wg:oauth:2.0:oob.

Add the following Redirect URI under Authentication (**Azure Active Directory > App registrations > stratafax** (name of the App you created) **> Authentication > Redirect URIs.** Under Type, select **"Public client (mobile & desktop)"** and enter **urn:ietf:wg:oauth:2.0:oob** under the Redirect URI.

Public Client (Mobile & Desktop): **urn:ietf:wg:oauth:2.0:oob**
Web: https://<customername>.stratafax.com/sso/saml/consumerservice.aspx


Redirect URIs

The URIs that we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs. Learn more about adding support for web, mobile and desktop clients

TYPE	REDIRECT URI
Public client (mobile & desktop)	urn:ietf:wg:oauth:2.0:oob
Web	https://staging.stratafax.com/sso/saml/consumerservice.aspx

Review certificate expiration data, status, and email notification

When you create a Gallery or a Non-Gallery application, Azure AD will create an application-specific certificate with an expiration date of 3 years from the date of creation. You need this certificate to set up the trust between Azure AD and the application. For details on the certificate format, see the application's SAML documentation.

From Azure AD, you can download the certificate in Base64 or Raw format. In addition, you can get the certificate by downloading the application metadata XML file or by using the App federation metadata URL. stratafax will need a copy of the Base64 certificate in order to setup the trust connection on the stratafax site.

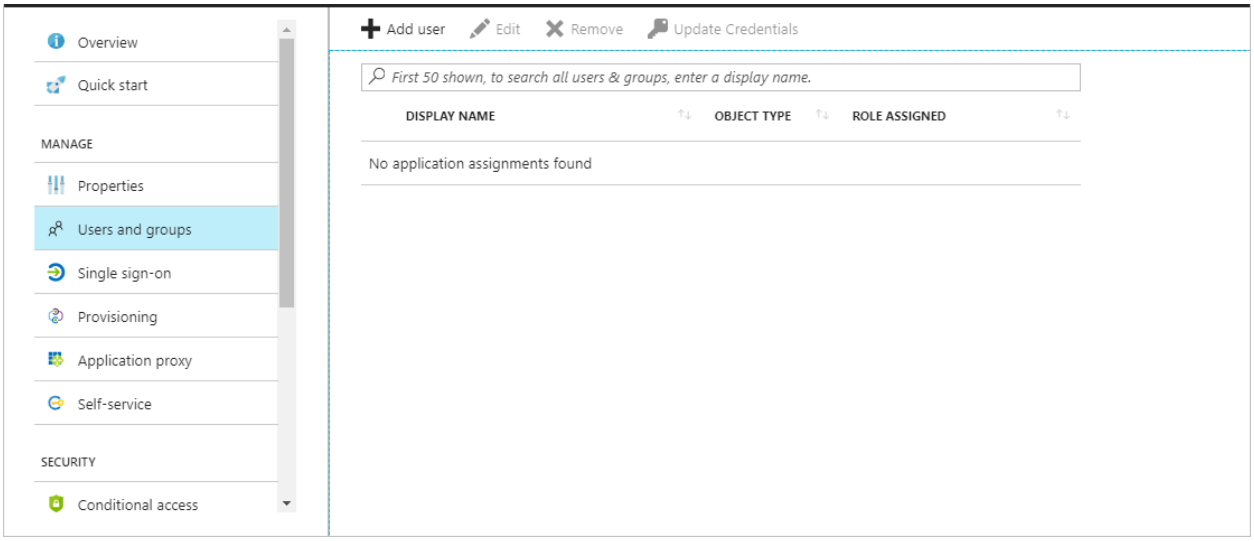
Set up stratafax application to authenticate through Azure AD

To configure stratafax for single sign-on, you will need to export the certificated in the previous section as Base 64 and provide this to support@stratafax.com. Once the certificate is enabled on the stratafax side, you can point your users to authenticate using the URL provided. The application will be listed under the Application menu when users log in to their Microsoft online account.

Assign users and groups to your stratafax SAML application

Once the **stratafax** application has been configured to use Azure AD as a SAML-based identity provider, then it is almost ready to test. As a security control, Azure AD will not issue a token allowing a user to sign into the application unless Azure AD has granted access to the user. Users may be granted access directly, or through a group membership.

To assign a user or group to your application, click the **Assign Users** button. Select the user or group you wish to assign, and then select the **Assign** button.



Assigning a user will allow Azure AD to issue a token for the user. It also causes a tile for this application to appear in the user's Access Panel. An application tile will also appear in the Office 365 application launcher if the user is using Office 365.

Test the SAML application

Before testing the SAML application, you must have set up the application with Azure AD, and assigned users or groups to the application. To test the SAML application, see How to debug SAML-based single sign-on to applications in Azure Active Directory.

stratafax user creation

Manual creation of users

There are two ways to created new users manually in stratafax.

- Create a user manually
- Import users from a file

Reference the stratafax Administrator's Guide for details on how to create users.

Synchronize users

If you enable external authentication for a user, you can enable synchronization of users through LDAP. A Secure LDAP connection is required through Azure AD or other internet accessible LDAP server in order to synchronize users.

stratafax Web Client and Printer Driver authentication with SSO

1. stratafax Web Client

Single Sign-on allows employees in a company to access all the company applications with one set of credentials. Depending on the company, the credentials can include email, phone number or username, along with the password. The company routes all logins through an IDP (Identity Provider) with which the company has a purchased license. The IDP usually hosts a login page for the employees to enter their company credentials before entering any application. Single Sign-on provides better security with the central authentication point, limiting the possibility of phishing.

QUICK TIP: To ensure there is no conflict with Single Sign-on for your account, each user contact email address must be unique when creating user extensions or call queue extensions.

2. stratafax Printer Driver

Stratafax Printer Driver version 3.2.0.2 or above is required for Microsoft SSO authentication.

stratafax IP Printer Download

The stratafax IP Printer can be downloaded from: stratafax IP Printer.exe

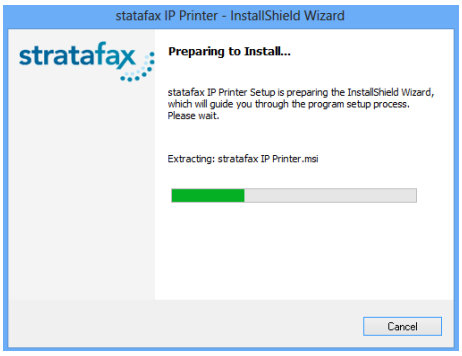
stratafax IP Printer Prerequisites

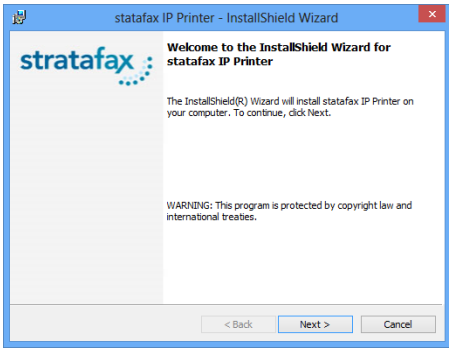
The stratafax IP Printer installation requires:

- Microsoft .Net 4.5. If you don't already have this installed on your desktop, you can download this from the Microsoft download page. (http://www.microsoft.com/en-us/download/details.aspx?id=30653
- Internet/network access to connect to the stratafax server.
- Stratafax username and password

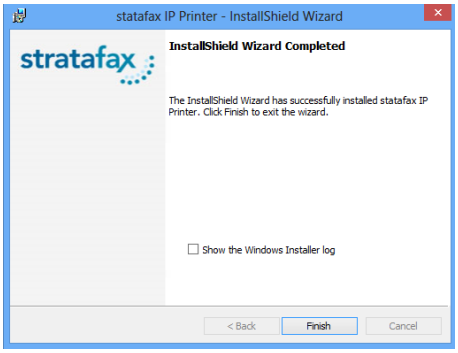
stratafax IP Printer Installation Instructions

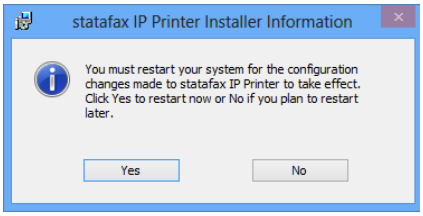
1. To begin installation, run "stratafax IP Printer.exe" and follow the on-screen instruction to complete the installation.



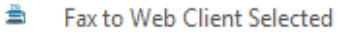


2. Click Finish once the installation completes and restart your system.





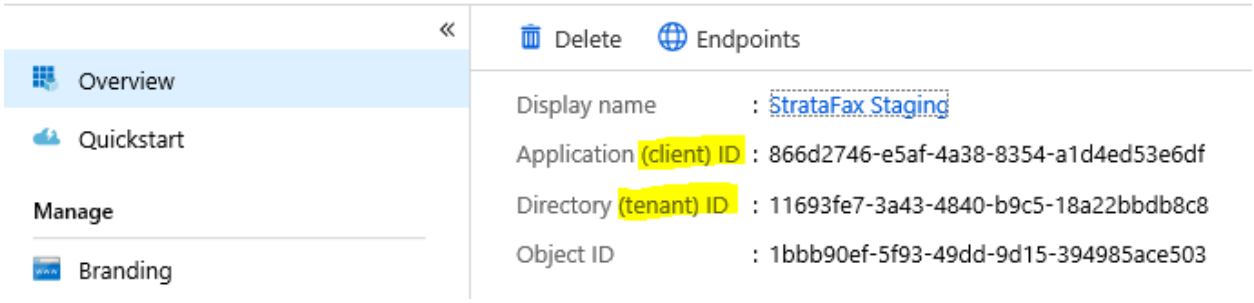
3. After you restart your system, you will see the following “Fax to Web Client” in the Windows taskbar.



4. After installation, you need to update the FXServers.config file in C:\stratafax\stratafax IP Printer to the following:

```
<?xml version="1.0" encoding="utf-8"?>
<FServers xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <FaxCoreServer>
    <fServer>
      <FaxCoreServerUrl>https://fax.stratafax.com/</FaxCoreServerUrl>
      <FaxCoreServerName>strataFax</FaxCoreServerName>
      <WindowsaAuthentication>false</WindowsaAuthentication>
      <SAMLSSO>true</SAMLSSO>
    </fServer>
  </FaxCoreServer>
</FServers>
```


5. Also update the WebPrint.exe.config file to match the AzureSSOClientID and AzureSSOTenantId from your Azure AD Application tenant. You can find this information under (**Azure Active Directory > App registrations > stratafax** (name of the App you created) **> Overview** (see example below).




```
<?xml version="1.0"?>
<configuration>
  <appSettings>
    <add key="urlMsgInterface" value="/printdriver/printdriverui.aspx"/>
    <add key="urlMsgPost" value="/printdriver/printdriverpost.aspx"/>
    <add key="urlWinMsgInterface" value="/printdriverwin/printdriverui.aspx"/>
    <add key="urlWinMsgPost" value="/printdriverwin/printdriverpost.aspx"/>
    <add key="urlSsoMsgPost" value="/printdriversso/printdriverpost.aspx"/>
    <add key="WinsAuth" value="0"/>
    <add key="server" value="fax.stratafax.com"/>
    <add key="port" value="443"/>
    <add key="isRaw" value="1"/>
    <add key="autoClose" value="0"/>
    <add key="https" value="1"/>
    <add key="lang" value="default"/>
    <add key="AzureSSOClientId" value="866d2746-e5af-4a38-8354-a1d4ed53e6df" />
    <add key="AzureSSOTenantId" value="11693fe7-3a43-4840-b9c5-18a22bbdb8c8" />
  </appSettings>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.6"/>
  </startup>
</configuration>
```

Note: One you modify and test the connection, these files can be copied to additional clients if you are deploying this to multiple workstations.

6. Check under Devices and Printers, for the newly installed printer called “stratafax IP Printer”.

7. Users can print to stratafax IP Printer from a native application such as Microsoft Word, Excel, Quickbooks, etc. to submit a fax to stratafax. Refer to **Using the stratafax IP Printer to Quickly Distribute Documents** for more details.

Using the stratafax IP Printer to Quickly Distribute Documents

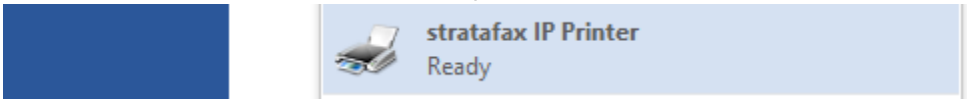
Once the stratafax IP Printer driver has been installed, you may print to it from within any application that allows printing. This means that any document (file) currently being worked may be distributed to recipients. It could be a Microsoft Word, Excel, PowerPoint, or Visio file. Actually, any application that offers the ability to print from is a good candidate.

The following is an example from within MS Word.

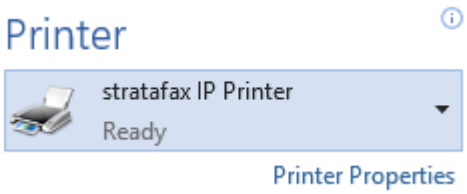
1. From the **File** menu choose **Print**. The **Print** dialog box shows.

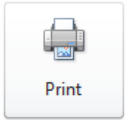
2. Click  to the right of the printer name currently showing.

3. Select **stratafax IP Printer** from the dropdown as shown below.



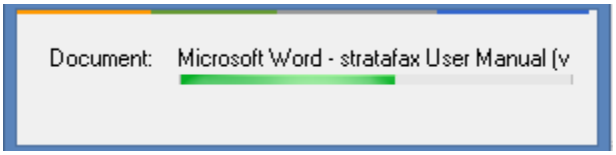
The **stratafax IP Fax Printer** is selected.



4. Click 

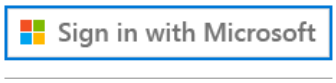
to close the **Print** dialog box and print using the selected print driver.

The document is preparing to print, but not to the local printer next to your desk or to the network printer in the workroom. Instead it is preparing to print using the **stratafax IP Printer driver**. This means it is preparing the file to be distributed to the list of recipients you select.

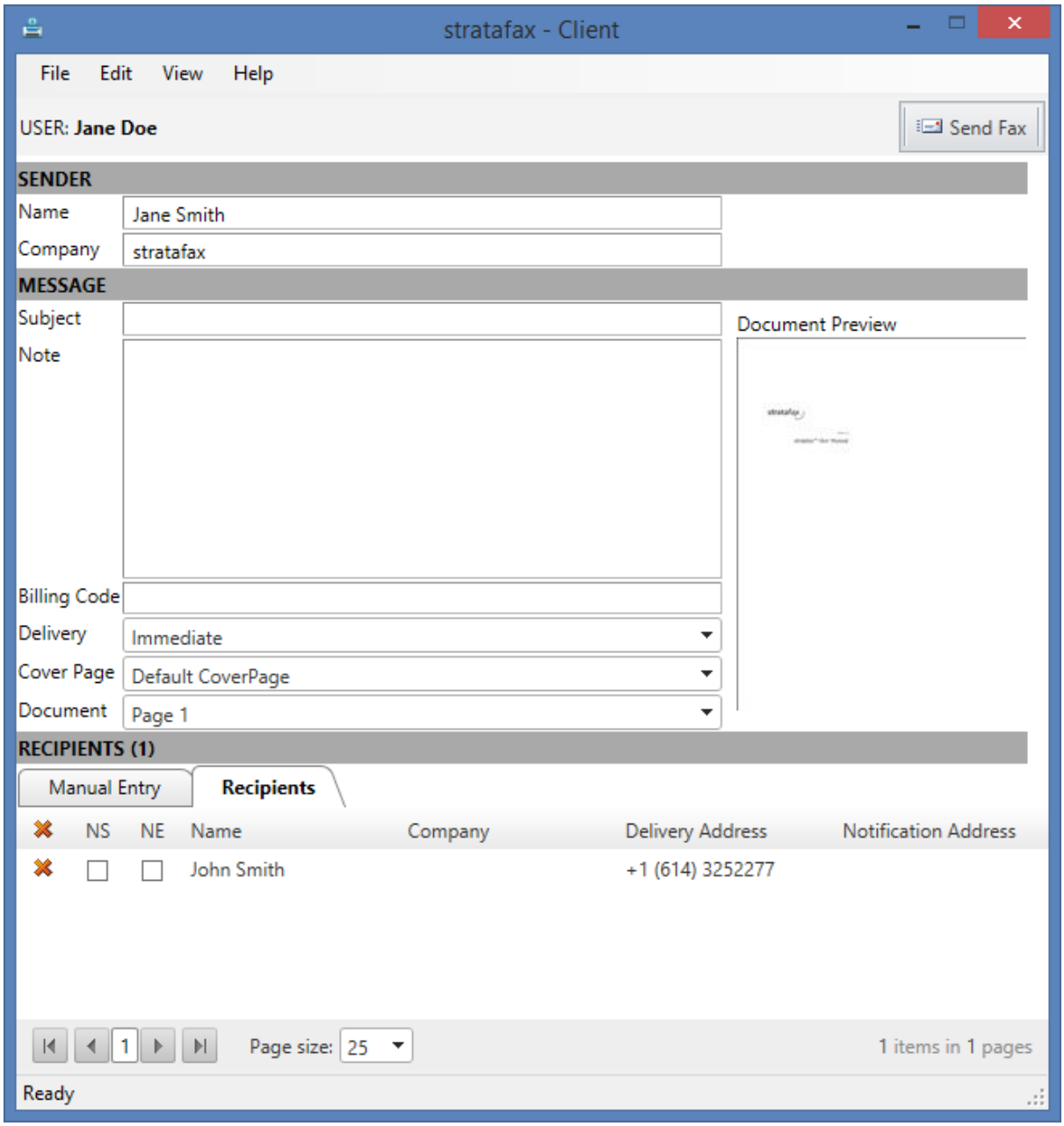


Once the **Preparing** message process is complete, the **stratafax Client Login** screen appears.

5. If this is your first time using the printer, you will be prompted to Trust this client. Select to **Sign in with Microsoft.**



6. Complete the necessary **Message** fields.
   Notice the first page of the document shows in the **Document Preview** area of the **stratafax 2007 – Client**.
   A **Billing Code** may be entered, if applicable.
   A **Delivery** type other than **Immediate** may be selected.
   The **Cover Page** will be provided by default; however, it may be disabled when necessary.



7. Enter the name of each recipient and click Add.
   Recipients may be selected from the **Address Book** or entered manually.
8. A **Tracking No.** may be included, if necessary.
9. Click Send Fax to distribute the selected document to the recipients.

About Instant InfoSystems

Instant InfoSystems is one of the world's most experienced value-added providers of cloud-based solutions for voice, fax, and data. For more than 25 years, we have solved complex challenges for Fortune 1000 customers in nearly every industry, helping organizations manage their critical documents, communications, and infrastructures more efficiently, intelligently, and securely. Today, Instant InfoSystems enjoys strategic relationships with the industry's leading developers of UCaaS, CCaaS, SD-WAN, and Fax technologies and provides a full spectrum of professional services, consultative guidance, and world-class technical support.

Contact Us

CORPORATE OFFICE
2301 West 190th Street, Suite 200
Torrance, CA 90504
Phone: 310.750.7200
Fax: 310.750.7210
info@instantinfo.com

SALES
Phone: 310.750.7200
Fax: 310.750.7210
sales@instantinfo.com

TECHNICAL SUPPORT
Phone: 310.750.7209
Fax: 310.750.7219
support@instantinfo.com

Follow Us

www.InstantInfoSystems.com

Facebook.com/instantinfosystems
Twitter.com/Instant_Info
Linkedin.com/company/Instant-InfoSystems

INSTANT INFO SYSTEMS
Information meets expertise.