



***OneLogin Integration***

***User Guide***

## Table of Contents

|   |    |
|---|----|
| OneLogin Account Setup.....                                   | 2  |
| <i>Create Account with OneLogin</i> .....                     | 2  |
| <i>Setup Application with OneLogin</i> .....                  | 2  |
| <i>Setup Required in OneLogin: SSO and AD Connector</i> ..... | 4  |
| OneLogin Website.....   | 4  |
| OneLogin Connector.....                                       | 7  |
| Return to OneLogin Website – Active Directory Setup.....      | 10 |
| Setup Required in ServicePRO application.....                 | 14 |
| <i>Provider tab</i> .....                                     | 16 |
| <i>Sync tab</i> .....   | 17 |
| <i>Verify tab</i> .....                                       | 18 |
| Prerequisites and Limitations.....                            | 19 |

## OneLogin Account Setup

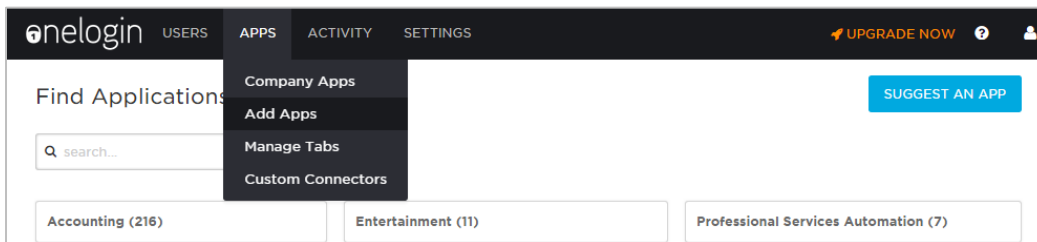
### Create Account with OneLogin

The following outlines steps for creating an account on OneLogin, and signing up for an account.

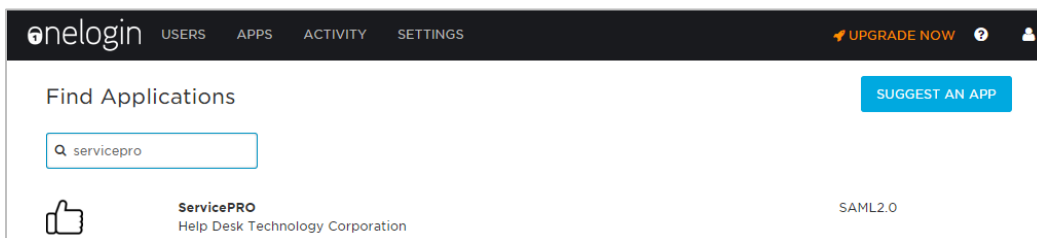
1. Go to OneLogin.com (or directly to <https://www.onelogin.com/signup?plan=free>)
2. Select Product, then Pricing
3. Select the option “SSO – Free (SSO for your employees for up to 3 apps and 5 personal apps)”
4. Enter your Name, Contact Info, Email Address and other information.

### Setup Application with OneLogin

1. Visit <https://app.onelogin.com/login> and login with the registered credentials.
2. From here, select **Apps – Company Apps > Add Apps**

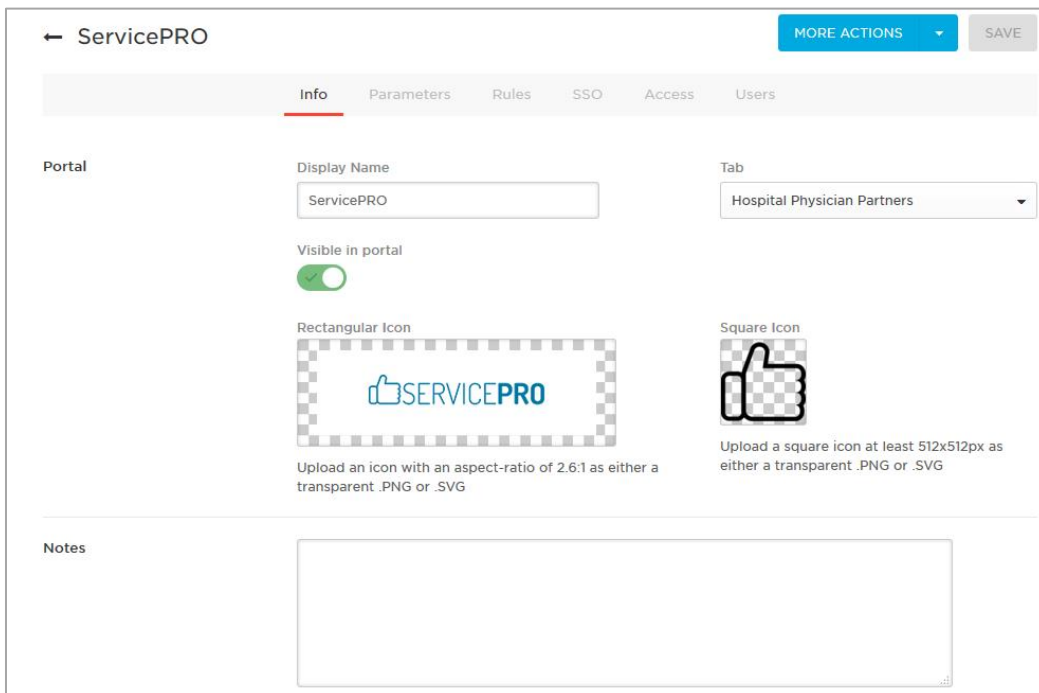


3. On this page, navigate to ServicePRO, or search for ServicePRO. Select **Add ServicePRO**.



4. On the Add ServicePRO page, check your basic settings and select **Save** from the upper right corner to save the configuration. You will be notified that your company has been added and taken to a page where you can edit additional settings.

- 5. On ServicePRO's page, leave all parameters at their default pre-configured settings unless changes are required.



The screenshot shows the configuration page for a ServicePRO portal. At the top, there is a navigation bar with a back arrow, the text "ServicePRO", and two buttons: "MORE ACTIONS" (with a dropdown arrow) and "SAVE". Below this is a horizontal menu with tabs for "Info", "Parameters", "Rules", "SSO", "Access", and "Users". The "Info" tab is currently selected and highlighted with a red underline.

The main content area is titled "Portal" and contains several settings:

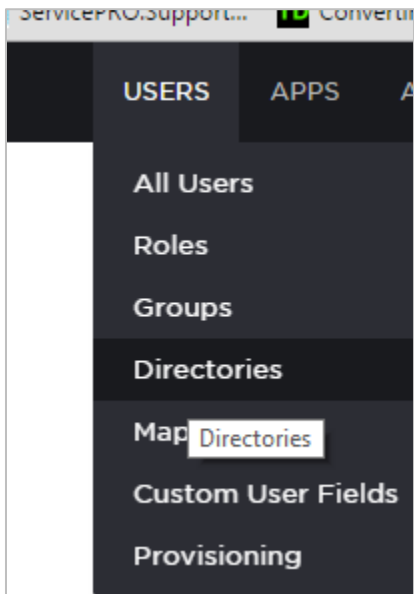
- Display Name:** A text input field containing "ServicePRO".
- Tab:** A dropdown menu currently set to "Hospital Physician Partners".
- Visible in portal:** A toggle switch that is turned on (green).
- Rectangular Icon:** A preview of a rectangular icon with a checkered background, containing the ServicePRO logo. Below it, the text reads: "Upload an icon with an aspect-ratio of 2.6:1 as either a transparent .PNG or .SVG".
- Square Icon:** A preview of a square icon with a checkered background, containing a thumbs-up icon. Below it, the text reads: "Upload a square icon at least 512x512px as either a transparent .PNG or .SVG".

At the bottom of the form, there is a section titled "Notes" with a large, empty text area for entering additional information.

## Setup Required in OneLogin: SSO and AD Connector

### OneLogin Website

1. Go to the **Users** tab and select **Directories**, then select the **New Directory** link.



2. Under **Select a Directory Type**, select **Active Directory**.

USERS APPS ACTIVITY SETTINGS

## Select a Directory Type

**What is a Directory?**  
A Directory is a central repository about your organization's user information that can be used to grant access to applications.

**Do you know?**  
OneLogin offers several options, for example, you can use Google Apps or OneLogin as a single directory. Multiple directories are also supported.

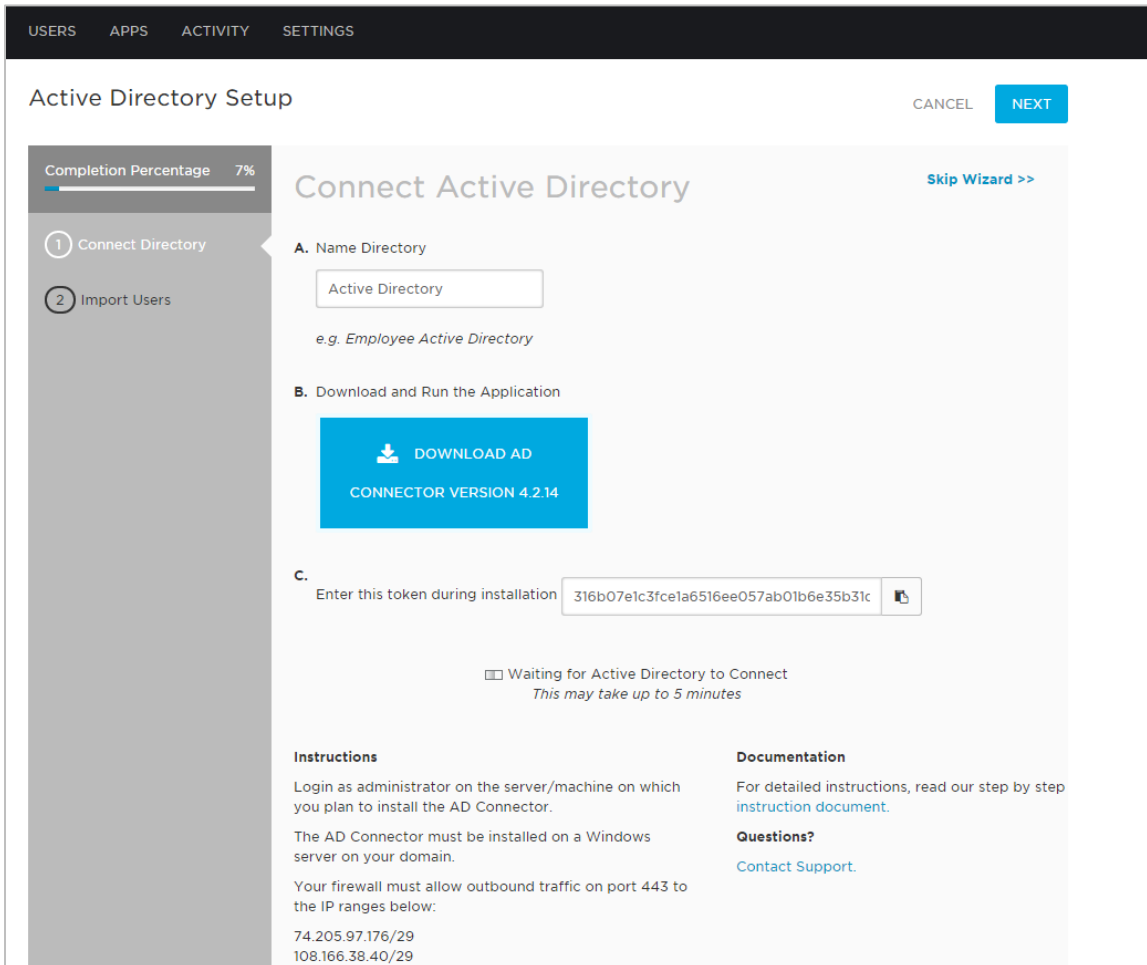
**ACTIVE DIRECTORY**

Install OneLogin's Active Directory Connector, which synchronizes users in real-time and enables authentication against AD. All communication is done over outbound SSL and does not require firewall changes.

Microsoft Active Directory

**CHOOSE**

3. Download and install the service from the **Connect Active Directory** page (onelogin\_ad\_connector.msi).  
Make note of the token text in Section C, as it will be required in a later step.



USERS APPS ACTIVITY SETTINGS

### Active Directory Setup

CANCEL NEXT

Completion Percentage 7%

## Connect Active Directory

Skip Wizard >>

1 Connect Directory

2 Import Users

**A. Name Directory**

Active Directory

e.g. Employee Active Directory

**B. Download and Run the Application**

DOWNLOAD AD  
CONNECTOR VERSION 4.2.14

**C. Enter this token during installation** 316b07e1c3fce1a6516ee057ab01b6e35b31c

Waiting for Active Directory to Connect  
This may take up to 5 minutes

**Instructions**

Login as administrator on the server/machine on which you plan to install the AD Connector.

The AD Connector must be installed on a Windows server on your domain.

Your firewall must allow outbound traffic on port 443 to the IP ranges below:

74.205.97.176/29  
108.166.38.40/29

**Documentation**

For detailed instructions, read our step by step [instruction document](#).

**Questions?**

[Contact Support](#).

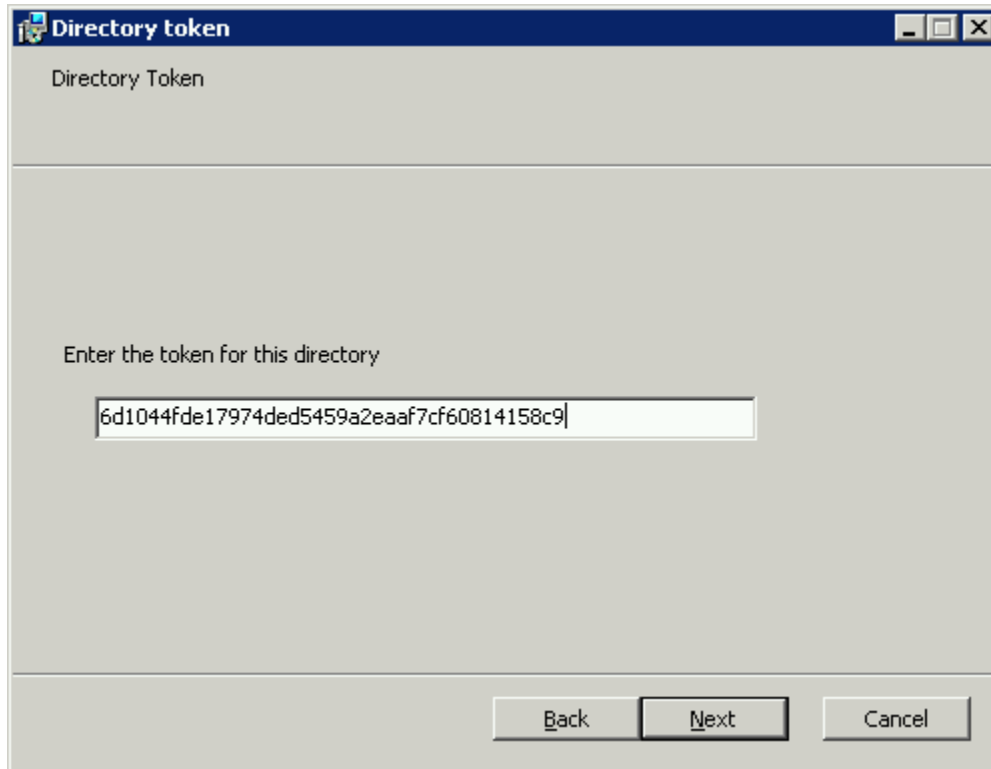
As stated on the Connect Active Directory page:

- Users should login as an Administrator on the server or machine where the AD Connector will be installed.
- The AD Connector must be installed on a windows server on your domain.
- Your firewall must allow outbound traffic on port 443 to the IP ranges below:
- 74.205.97.176/29
- 108.166.38.40/29

## OneLogin Connector

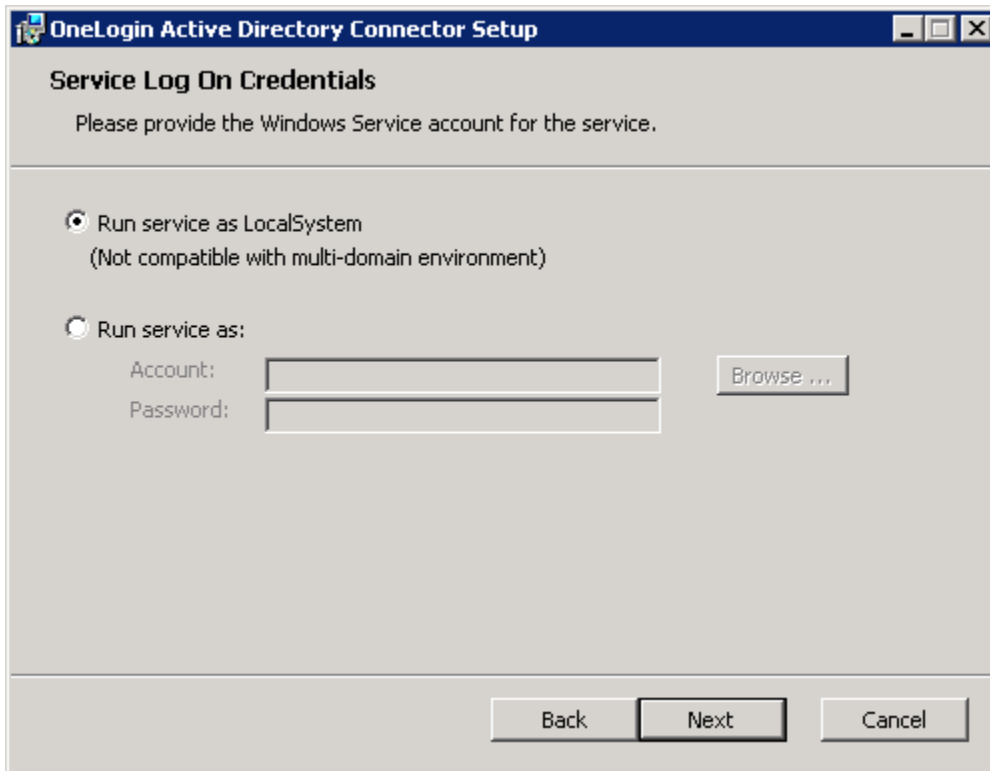
Open the OneLogin Connector (onelogin\_ad\_connector.msi) from its location to set up the Active Directory Connector.

1. For the **Directory Token**, copy the text in the Token field from section C of the Active Directory Setup page (Step 3-4).

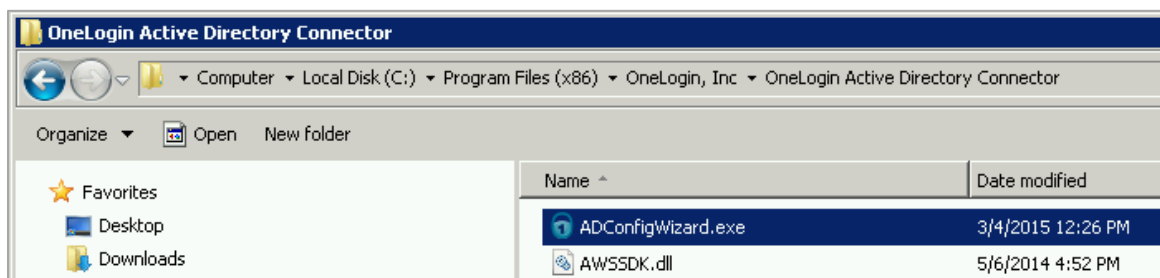




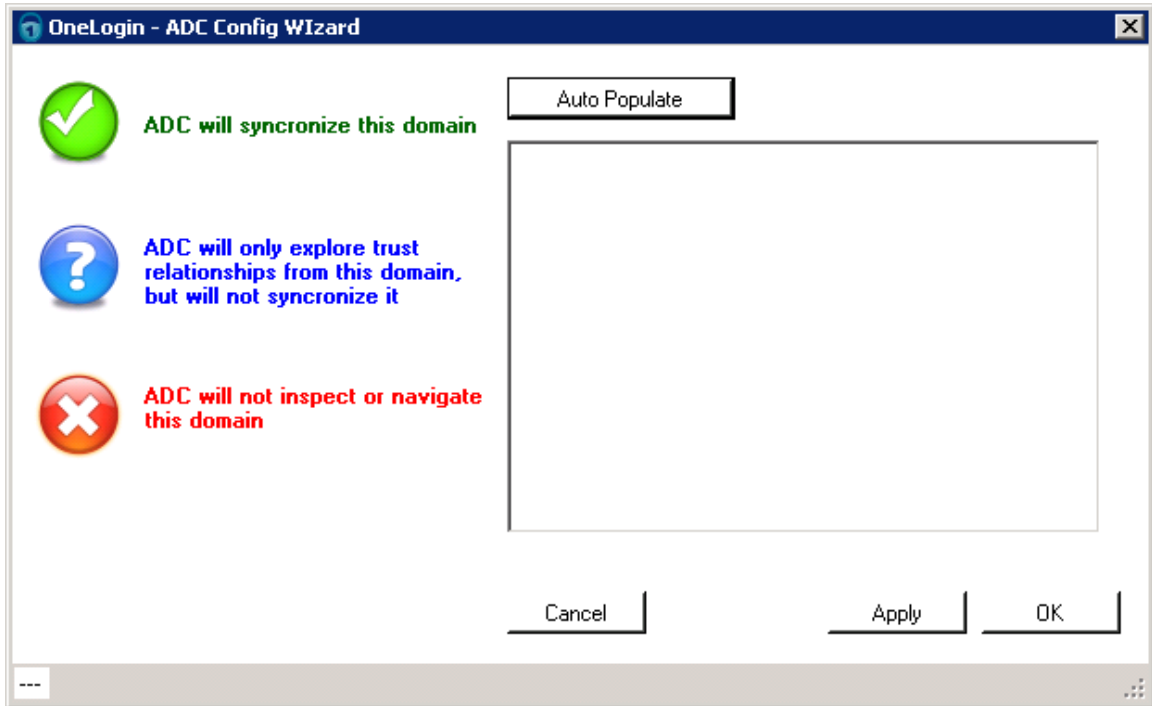
1. For **Service Log On Credentials**, select **Run service as LocalSystem**.



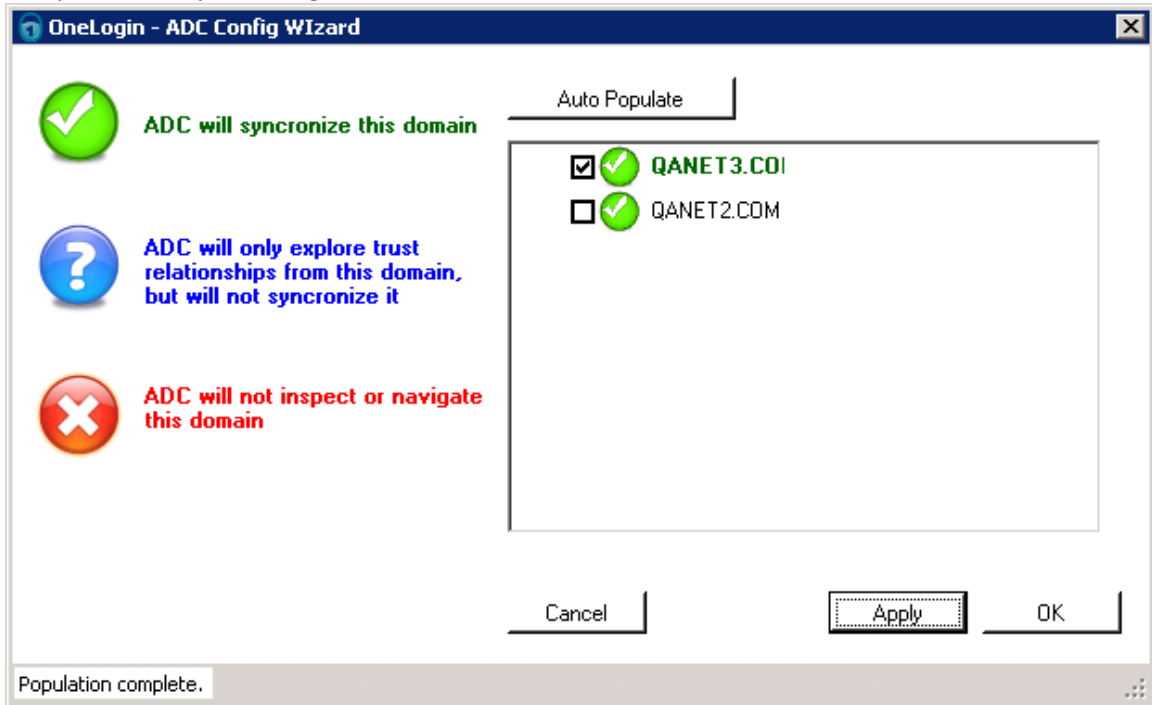
2. For **Port Selection**, the value can be left as the default (8080), provided there are no port conflicts with the current setup.
3. Once installed, the **OneLogin Active Directory Connector Setup** window will open. If needed, users can change or access the ADC Config Wizard by opening **ADConfigWizard.exe** from the directory where it is installed.



- In the **OneLogin – ADC Configuration Wizard**, select **Auto Populate** to populate the list with available domains.



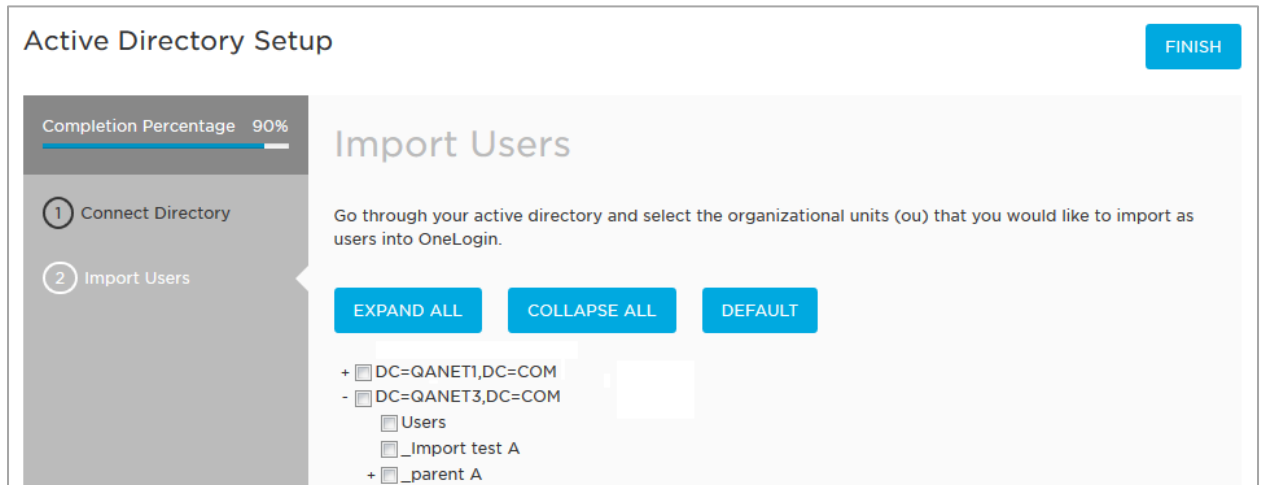
- Check off domains you wish to use in Active Directory setup. Select **Apply** or **OK** and close the setup window by selecting **Finish**.



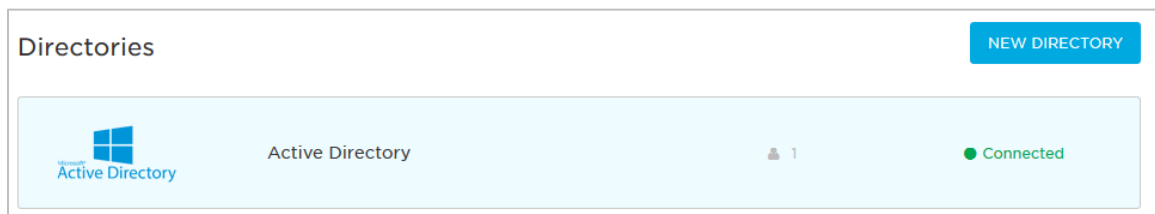
## Return to OneLogin Website – Active Directory Setup

After completing the steps in the OneLogin Connector Setup, return to the Active Directory Setup page in the browser. The page will refresh and the page will display the **Import Users** screen.

1. Select the checkboxes for the desired Organizational Units in your Active Directory.



2. Select **Finish** from the upper right corner when appropriate users have been selected. The Connectors list page will be loaded.
3. To begin mapping, select **Users** dropdown menu, then select **Directories**. On the Directories page, select **Active Directory**.



**NOTE:** Users will require valid email address for logins to appear in the Active Directory list.

- To sync a user, navigate to the **More Actions** icon in the upper right, and select **Synchronize Users**. A prompt will appear, confirming “The connector is synchronizing users.”

Active Directory

Connector Instances | OU Selection | Directory Attributes | Ad

MORE ACTIONS | SAVE

Delete

Synchronize Users

Active

ADC ● connected 4.2.14

Standby

ⓘ It looks like you do not have any Active Directory failovers configured.

For an optimum experience, set up multiple Active Directory Connectors to access your directory. If one of your connectors fails to connect with OneLogin's servers, our systems will automatically try all of the ADC failovers you set up and have on standby.

+ADD A CONNECTOR FAILOVER

No, thank you. I will add one later.

- View the User listing from **Users > All Users**.  
If Users do not appear in the listing, ensure the user in the Organizational Unit is associated with an active email address in its Active Directory properties.

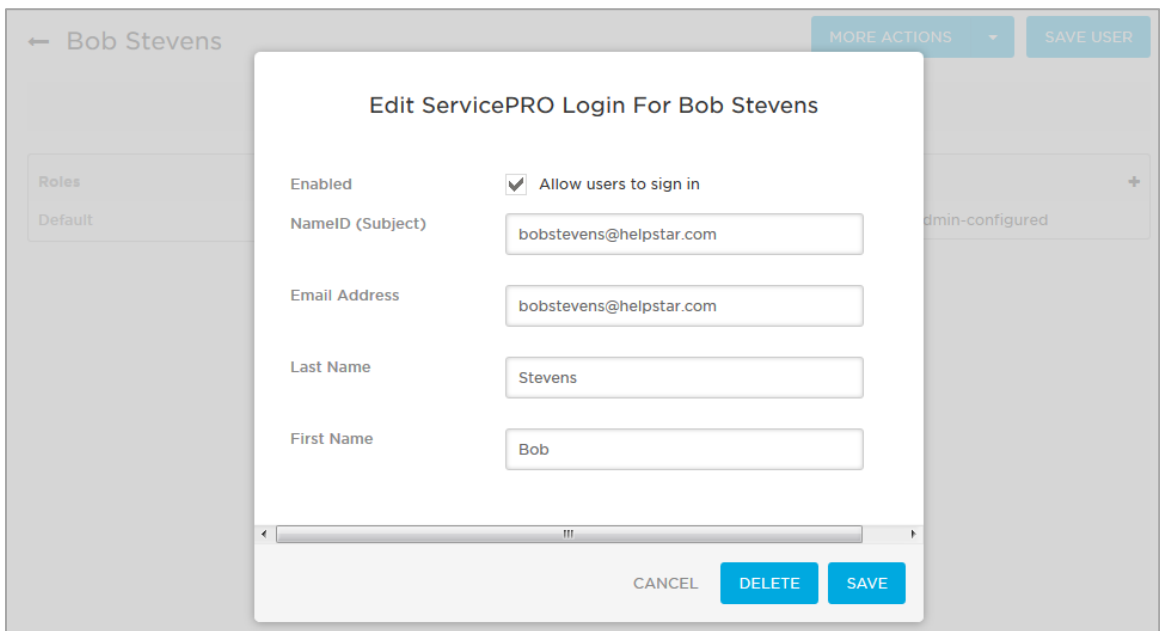
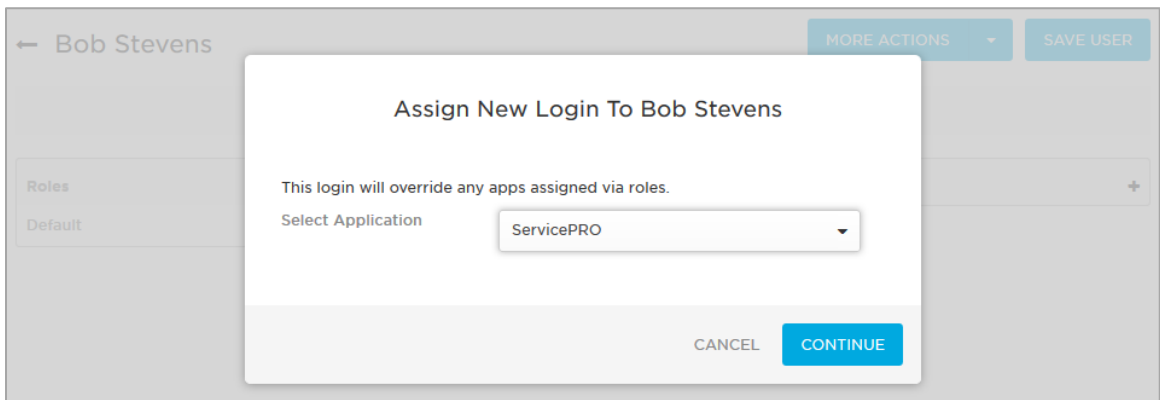
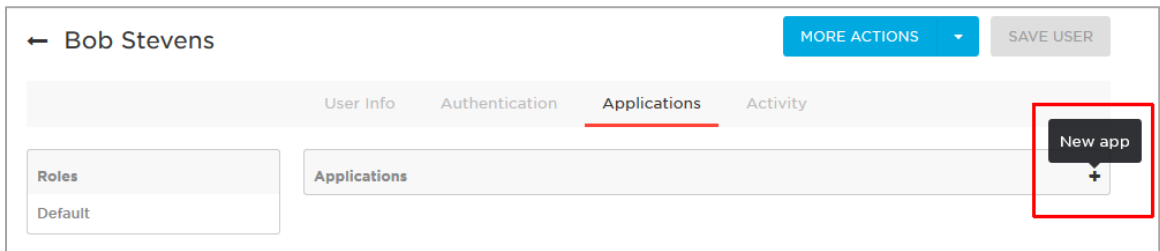
| Name        | Type | Description |
|-------------|------|-------------|
| Jim Johnson | User |             |
| Joe Johnson | User |             |
| OneLoginQA  | User |             |

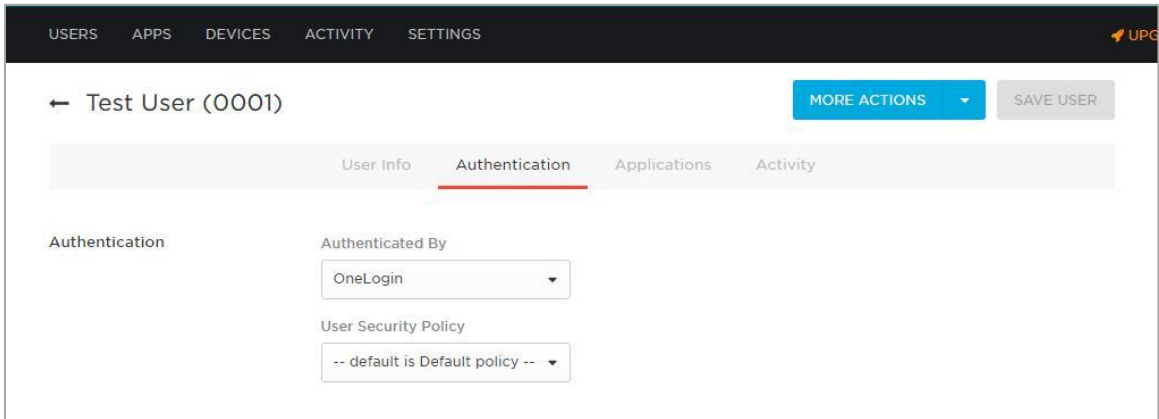
Jim Johnson Properties ? X

|                          |   |   |                      |            |
|--------------------------|---|---|----------------------|------------|
| Published Certificates   | Member Of   | Password Replication                    | Dial-in              | Object     |
| Security                 | Environment   |   | Sessions             |            |
| Remote control           | Remote Desktop Services Profile   |   |                      |            |
| Personal Virtual Desktop | COM+  | Attribute Editor                        |                      |            |
| <b>General</b>           | Address   | Account                                 | Profile              | Telephones |
| Jim Johnson              |   |   |                      |            |
| First name:              | <input type="text" value="Jim"/>  | Initials:                               | <input type="text"/> |            |
| Last name:               | <input type="text" value="Johnson"/>  |   |                      |            |
| Display name:            | <input type="text" value="Jim Johnson"/>  |   |                      |            |
| Description:             | <input type="text"/>  |   |                      |            |
| Office:                  | <input type="text"/>  |   |                      |            |
| Telephone number:        | <input type="text"/>  | <input type="button" value="Other..."/> |                      |            |
| E-mail:                  | <input style="border: 2px solid red;" type="text" value="jjohnson@qanet3.com"/> |   |                      |            |
| Web page:                | <input type="text"/>  | <input type="button" value="Other..."/> |                      |            |

- To set up Mapping to your domain for a User, select the name from the User listing, and select the **Applications** tab, and add a New App. Ensure **ServicePRO** is selected as the application, and choose the correct ServicePRO Login information for the user. Ensure the connector service on the machine on your domain is set up (see steps above).



7. Confirm the 'Authenticated By' setting for users is correctly set to 'OneLogin'.



# Setup Required in ServicePRO application

While authenticating via OneLogin, login is only possible via email address.

To authenticate OneLogin’s Single Sign-on settings in ServicePRO:

1. From the ServicePRO Workbench, select Setup/Administration.
2. From here, navigate to the Configuration Tab.
3. Select System Options.
4. Select the Single Sign-on Settings option on the left side bar.
5. Enable Single sign-on functionality and edit details below by selecting the first checkbox option.

The screenshot shows a web application window titled "ServicePRO System Options" with a sub-tab "Single Sign-on Settings". The window includes a sidebar with navigation options: General, System Defaults, Calendar Synchronization, Generic Types, Service Level Agreement, Purchase Order Options, Refresh Timer Settings, and Single Sign-on Settings (which is highlighted). The main content area is titled "Single Sign-on settings" and contains the following configuration options:

- Use Single sign-on in ServicePRO?
- Use Single sign-on in Self-service portal?

Below these are several input fields:

| Provider   | Sync | Verify |
|--|------|--------|
| Provider: OneLogin   |      |        |
| Login URL: https://serviceproqa.onelogin.com/api/v3/saml/assertion |      |        |
| OneLogin API Key: 6348abd6dd1858eaeaf41b91e70af374cac5364          |      |        |
| OneLogin APP Id: 455299  |      |        |

At the bottom of the configuration area, there is a checked checkbox:  Automatically create user in Self-service portal?

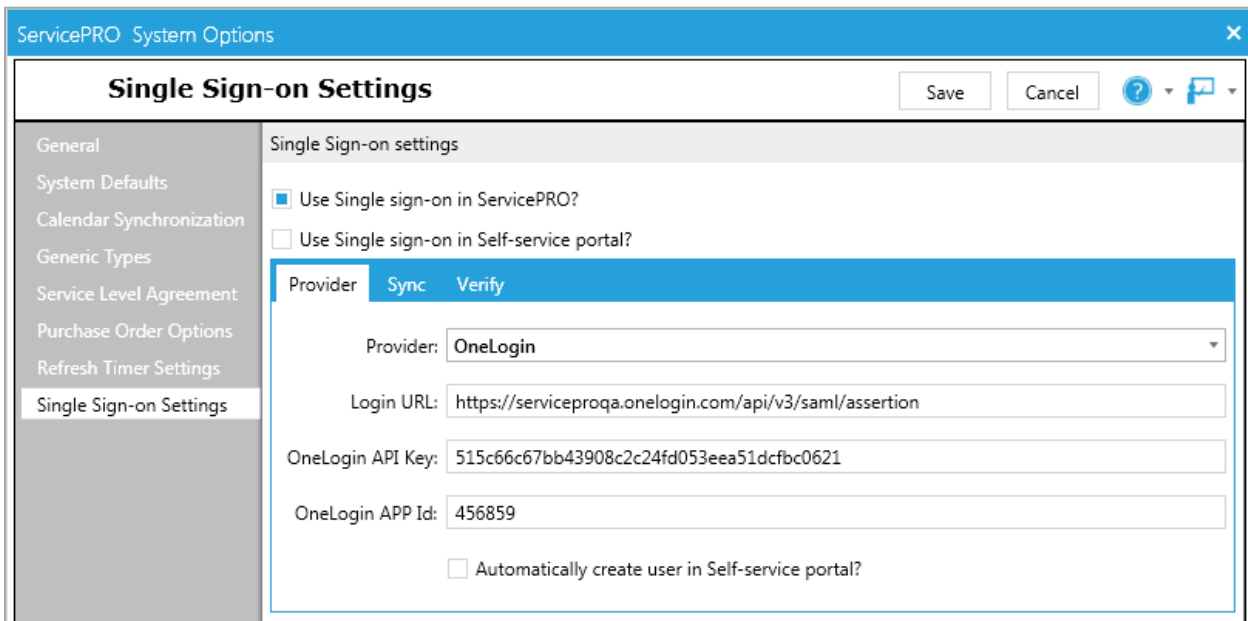
Buttons for "Save" and "Cancel" are located at the top right of the configuration area.



## Provider tab

The following options are available under the Single Sign-on Settings page's Provider tab. Information for each field can be found on OneLogin's website, as noted in each section below.

- **Provider:** OneLogin
- **Login URL:** The first part of the URL will be unique for each client
  - [https://\[unique identifier\].onelogin.com/api/v3/saml/assertion](https://[unique identifier].onelogin.com/api/v3/saml/assertion)
  - In the example below, **serviceproqa** is the unique section of the URL
- **API Key:** REST API Key from OneLogin
  - The API Key can be found at [https://admin.us.onelogin.com/session\\_settings](https://admin.us.onelogin.com/session_settings), under API Key.
- **App ID:** The ID in Issuer URL is unique per client, and is visible when viewing Company App pages.
  - Using this URL as an example: <https://admin.us.onelogin.com/apps/456859/edit>  
The APP ID would be **456859**.
- **Automatically create user in self-service portal option:** If checked, will sync the user from OneLogin to ServicePRO



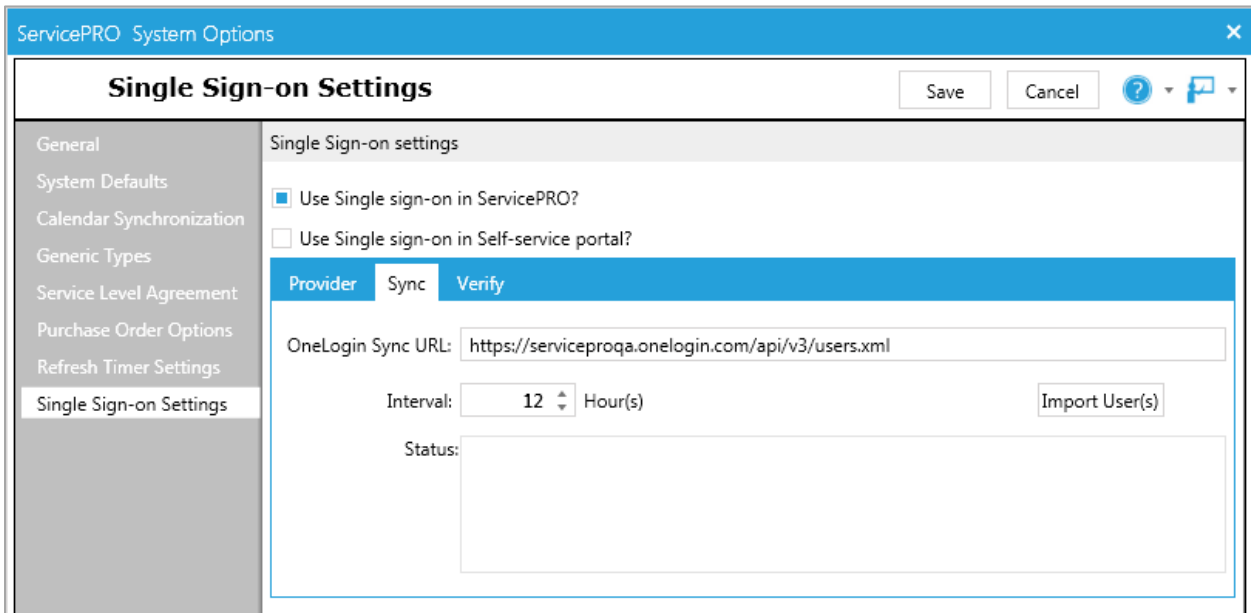
The screenshot shows the 'Single Sign-on Settings' page in the ServicePRO System Options interface. The 'Provider' tab is selected, and the settings are as follows:

| Provider          | Sync  | Verify                   |
|-------------------|---|--------------------------|
| Provider:         | <input checked="" type="checkbox"/>   | <input type="checkbox"/> |
| Login URL:        | <a href="https://serviceproqa.onelogin.com/api/v3/saml/assertion">https://serviceproqa.onelogin.com/api/v3/saml/assertion</a> |                          |
| OneLogin API Key: | 515c66c67bb43908c2c24fd053eea51dcfbc0621  |                          |
| OneLogin APP Id:  | 456859  |                          |
|                   | <input type="checkbox"/> Automatically create user in Self-service portal?  |                          |

## Sync tab

The following options are available under the Single Sign-on Settings page's Sync tab.

- **Sync URL:** The first part of the URL will be unique for each client
  - `https://[unique identifier].onelogin.com/api/v3/users.xml`
  - In the example below, **serviceproqa** is the unique section of the URL
- **Interval:** Set the frequency for User Imports from OneLogin by Starwatch Service, in hours
- **Import Users button:** Manually import users from OneLogin
- Fields that are synced upon User Import will include Email Address, User Name & Status (*active* or *inactive*)



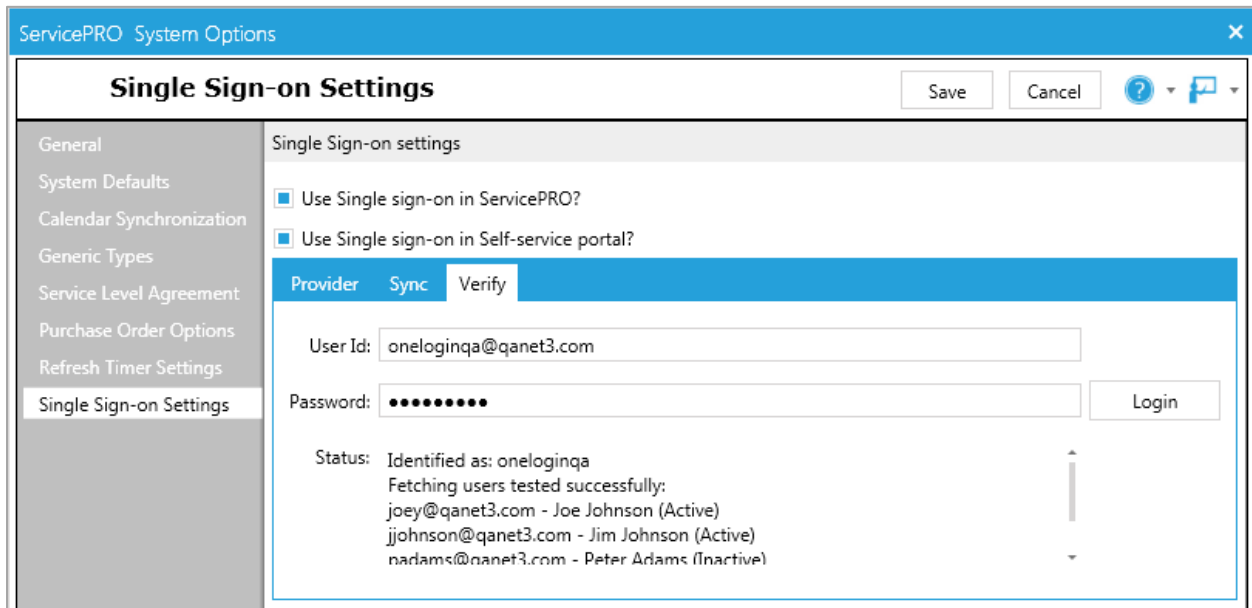
The screenshot shows the ServicePRO System Options window with the Single Sign-on Settings page open. The Sync tab is selected, and the following settings are visible:

- Single Sign-on settings**
  - Use Single sign-on in ServicePRO?
  - Use Single sign-on in Self-service portal?
- Provider** | **Sync** | **Verify**
- OneLogin Sync URL: `https://serviceproqa.onelogin.com/api/v3/users.xml`
- Interval:  Hour(s)
- Status:

## Verify tab

Users can use these options to verify the status of their OneLogin User IDs by entering the requested information.

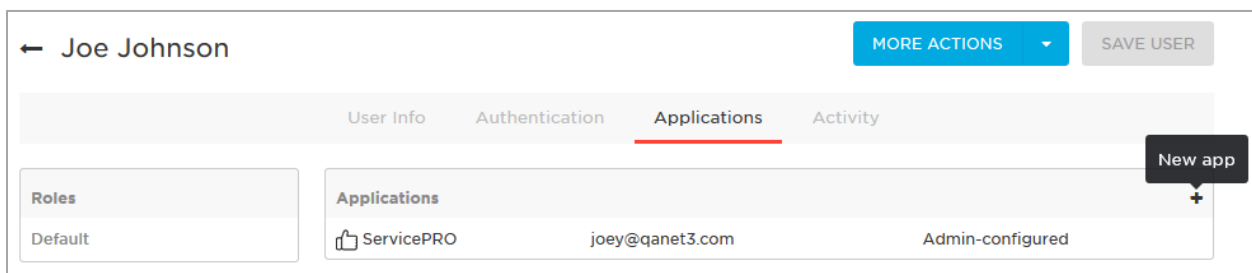
- **User Id:** Enter the User Id for the account to be used with OneLogin
- **Password:** Enter the Password associated with the User Id account
- **Login:** Test the OneLogin functionality
- **Status:** States the status of the logged in user



To log in as a User for the verification process, ensure that the User has accounts set up properly on both ServicePRO and OneLogin. This includes:

- Setting up User accounts with Manage Users (if not present) in ServicePRO
- Ensuring the User is associated with the ServicePRO application in OneLogin (See **Step 6** in the section **Return to OneLogin Website – Active Directory Setup**)

In the example below, the User “Joe Johnson” has the ServicePRO app added to their list of applications on the User Page in OneLogin.



## Prerequisites and Limitations

### 1. UserID

Single sign-on (SSO) with OneLogin requires an email address (a primary SMTP email address) for User IDs when logging in. UserID or UserName cannot be used to log in, as OneLogin's free plan does not allow these fields to be mapped.

### 2. Set Active Directory Authentication Method

In order for SSO to begin working, Administrators will need to ensure all users imported from the Active Directory has the Active Directory authentication method set.

### 3. Passthrough Authentication

Passthrough Authentication is not possible with SSO using OneLogin.

### 4. User Synchronization (Importing Users from OneLogin)

An alternative method for user provisioning is currently being used; the current API is not officially supported by OneLogin for User Import from Active Directory via OneLogin. As a result, restrictions on User Synchronization will be present:

- Only approximately 1000 users may be imported
- Field mapping can only be performed on User Name and Email Address fields
- Imported users will need to be assigned to a default organizational unit. Administrators will be able to adjust the user properties at a later point if needed.