Introduction to SSO for Jobpac Connect with ViewpointOne ID

If you have a ViewpointOne enabled subscription to Jobpac Connect it is possible to activate SSO (Single Sign On) for your Jobpac Connect Users. You will need to migrate users who wish to take advantage of SSO from their current Jobpac Connect User Profile, or **Jobpac ID,** to a **ViewpointOne ID**.

Migrating your users to a ViewpointOne ID will firstly allow your users to navigate seamlessly between Jobpac Connect and other components of the ViewpointOne connected construction solution suite. Additionally, it will allow integration with Azure Active Directory (Azure AD) to manage user access and enable single sign-on (SSO) to ViewpointOne. By integrating with Azure AD and using SSO, you can log into ViewpointOne using a consistent and secure process defined by your company from any supported device.

This document describes the process of migrating your Jobpac Connect users to a ViewpointOne ID and integrating with Azure.

Contents

Three Steps to enable SSO for your Jobpac Connect users

The enablement of SSO for your Jobpac Connect users and the integration to Azure AD is a three step process. It is important to note that SSO between ViewpointOne Solutions can be configured without integrating to Azure AD if desired.

1. Contact Viewpoint Support for a representative to configure single sign on for ViewpointOne.
2. Add ViewpointOne in the Azure Active Directory Portal (if this is your requirement)
3. Migrate your Jobpac Connect Users to a ViewpointOne ID (this can be done individually, or in bulk)

NOTE: We advise that you invite users in a contolled way, smaller groups is best so that you can stay on top of feedback and refine process. We also advise that you give users warning and some education prior to activation.

Once you have integrated ViewpointOne SSO with Azure AD, you can:

- Use Azure AD to manage user access and enable single sign-on with ViewpointOne.
- Use the Azure portal to manage your accounts in a centralized location.
- Enable your users to be automatically signed-in to ViewpointOne SSO with their Azure AD accounts.

Step 1: Contact Viewpoint Support to configure SSO for Viewpoint One

To configure single sign on for ViewpointOne, contact the Viewpoint Support team and provide your target domain name (for example, viewpoint.com) through which you are logging into ViewpointOne.

Please log on to the Viewpoint Support Portal to contact Viewpoint Support. A Viewpoint Support representative will configure single sign on for your enterprise in ViewpointOne, and then notify you when it's time to add ViewpointOne in the Azure Active Directory portal.

Step 2: Add ViewpointOne in the Azure Active Directory Portal

Please follow the following link to a help topic for integrating with Azure AD: https://help.viewpoint.com/viewpoint-team/viewpoint-team/administration/about-integrating-with-azure-ad.

As an additional resource, at the bottom of this KB Article is a short tutorial where you learn how to integrate ViewpointOne with Azure Active Directory.

Step 3: Migrate Jobpac Connect Users to a ViewpointOne ID

In this section we will describe the process of activating SSO for a Jobpac Connect user profile by migrating them to a ViewpointOne ID.

*NOTE: It is important that your users have their email address setup in Jobpac and this should be an email address within your company domain. You can check user email addresses using the **eContacts Maintenance** program in the Jobpac Administration Menus*

Migrating an individual Jobpac Connect user profile to a ViewpointOne ID

It is possible to activate users Individually for SSO. To do this you can Invite them individually as described below. See subsequent section in this document to see how users accept an Invitation to use their new ViewpointOne ID.

1. Navigate to the **Enrol Users in CMS** program from the System Administration menu

2. Select a user to activate for SSO with a **Right click**
3. Take the option to **Invite user to VP1 SSO** (as shown below). This will send the selected user an email invitation to setup their new ViewpointOne ID (Note, this may take some time)
4. You will notice the text change colour to pink once the user has been invited and this may take a few seconds.

NOTE: Users will not be able to use their Jobpac ID from this point forward and must accept their ViewpointOne invitation and use it to log in to Jobpac Connect.

Migrating Jobpac Connect user profiles in Bulk to ViewpointOne ID's

In this section we will describe how to invite users in bulk to use a ViewpointOne ID. We advise small batches of users so that you can control education and feedback with minimal disruption, and also due to the processing time for large batches of user invitations. We recommend that you calculate the processing time for one user invitation and then extrapolate, before deciding how many users to invite in bulk. Consider session inactivity timeouts set to 30 mins.

1. Navigate to **Enrol Users in CMS** from the System Administration menu
2. **Use filters** to select a range of users if required
3. Take the Action option to **Invite All to VP1 SSO** (as Shown Below) This step will invite all filtered users and will not reinvite users who have already been activated
4. You will notice the text change colour to pink once the user has been invited and this may take some time.

NOTE: Users will not be able to use their Jobpac ID from this point forward and must accept their ViewpointOne invitation and use it to log in to Jobpac Connect.

Deactivating SSO for a Jobpac Connect user

There may be situations where you would like to deactivate a user from SSO. Deactivating a user will remove their ViewpointOne ID and they will be able to use their old Jobpac ID profile to sign on

1. Navigate to **Enrol Users in CMS** from the System Administration menu
2. Select a user to deactivate for SSO with a **Right click**
3. Take the option to **Deactivate SSO** (as shown below). Their profile should go back to black or green depending on their existing links to the Viewpoint One Team for Project Management Product.
   Ie. a user can be "linked" to the Viewpoint One platform but continue to use their Jobpac ID to sign on to Jobpac. This Type of user will be able to use the dep links from our Project Management Platform but will not be able to use SSO.

How to Accept an Invitation to your new ViewpointOne ID

Users Invited to become ViewpointOne SSO users will receive an email invitation that looks like below with your Company logo and it will come from DoNotReply@viewpoint.com. The user will need to follow the prompts to confirm email and configure their account. Consider Spam settings if looking for lost invitations.

The screen shots below describe the user experience and workflow for accepting an invitation to ViewpointOne.

1. A ViewpointOne Invitation will look something like below with your logo.

2. Following the prompts, the user will see a similar screen to below where they will set up their details. These credentials are linked to the user company email address. The password should reflect your SSO password. Note this may behave differently depending on your Azure AD settings but essentially the user follows the on screen prompts.

VIEWPOINT

Email Address - *You'll use this to sign in*

andrew_tucker+tuck1@trimble.com

Organization - *You can change this once your account has been registered.*

None Yet

First Name *

Tucker

Last Name *

One

Phone

🇺🇸 ▼ (555) 555-5555
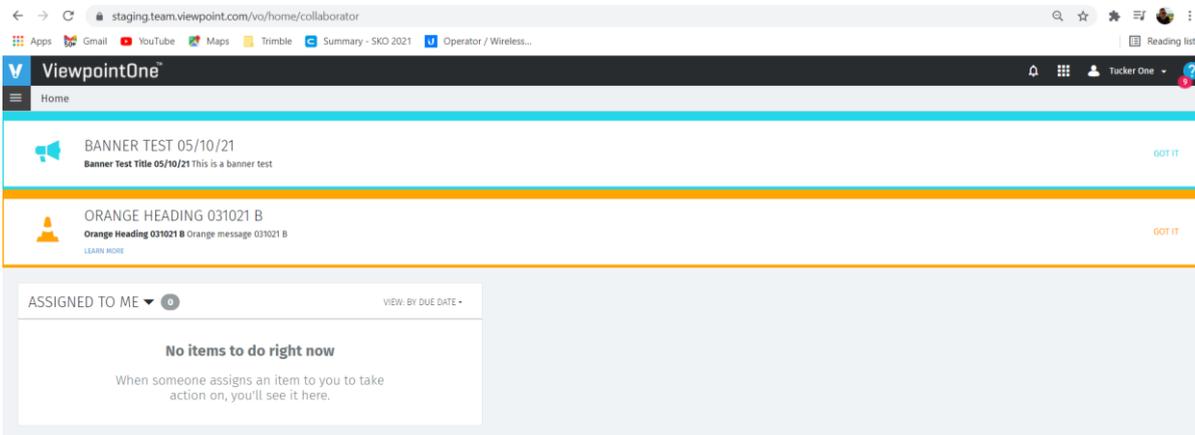
Password

•••••••••••   SHOW

Password must contain:
- ✅ At least 10 characters
- ✅ At least 1 uppercase letter
- ✅ At least 1 lowercase letter
- ✅ At least 1 number
- ✅ At least 1 special character

CREATE ACCOUNT   Already have an account? Click here to sign in.

VIEWPOINT
A TRIMBLE COMPANY

3. As the final stage of ViewpointOne activation, the user will end up on the ViewpointOne Landing Page as shown below. If you are not using other components of ViewpointOne, such as Viewpoint Team for Project Management, then this screen will seem a little unfamiliar and the User can just close the tab and launch a Jobpac Session with their ViewpointOne ID.
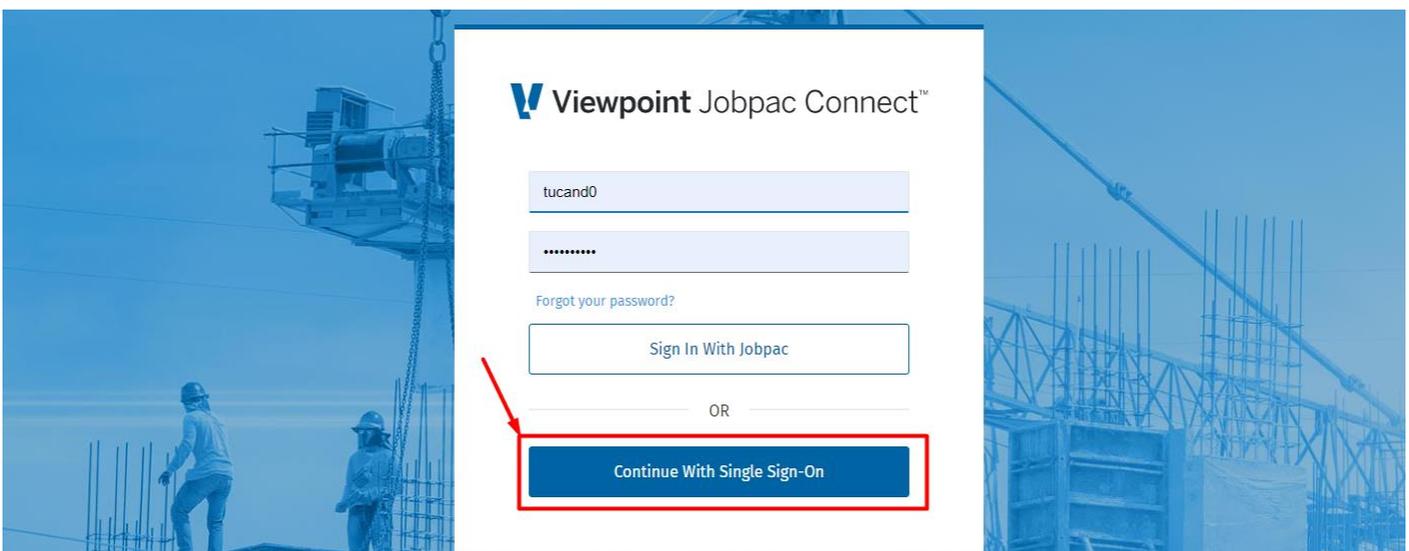

How to sign-on to Jobpac Connect with your new ViewpointOne ID

You will note in the screenshot below that in environments configured for SSO, users will be given the option of Signing-In with either their Jobpac ID or their ViewpointOne ID.
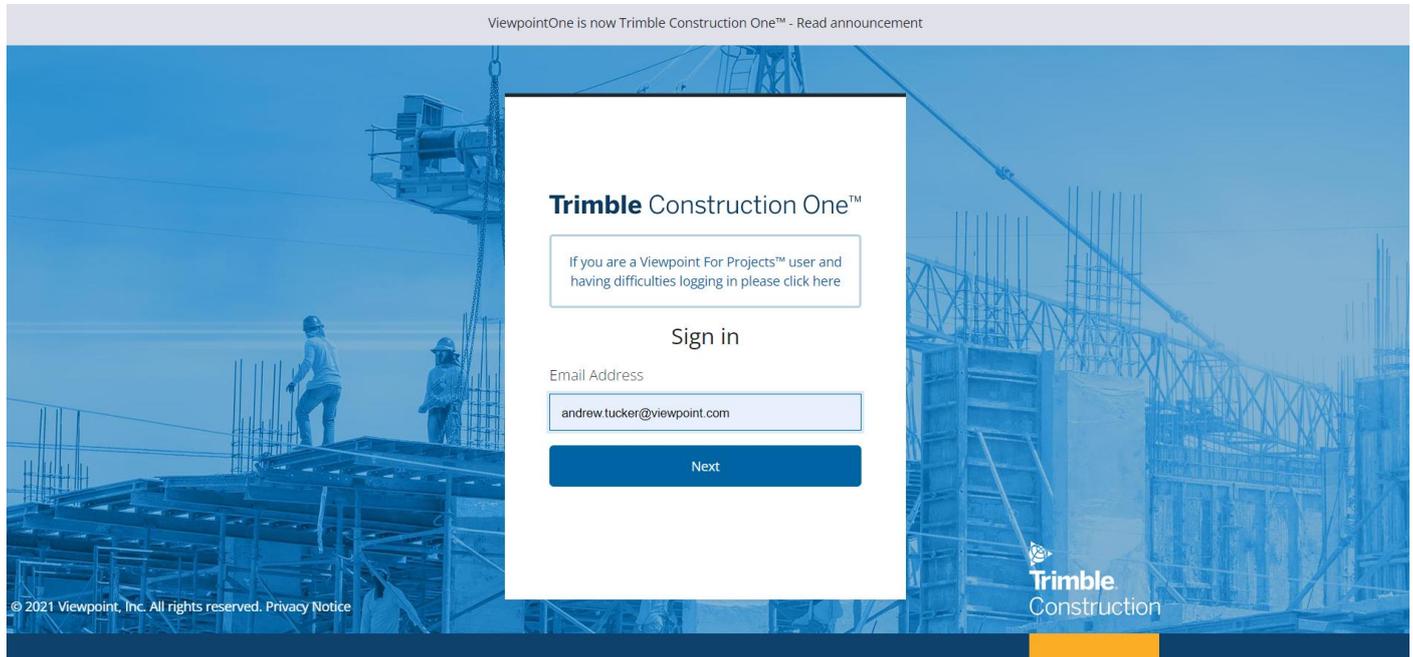
While transitioning to full SSO you may have some users with a new ViewpointOne ID and some users who still use their Jobpac ID. Both sign-in options are available on the login page, as you can see below, but a user will only be able to use the type of ID that is applicable to them. That is, once a user is migrated to a ViewpointOne ID then the Jobpac ID becomes redundant for that user (unless SSO is deactivated.)

Once a Jobpac Connect user has been given a ViewpointOne ID they will not need to use their old Jobpac ID. And they should click the **Continue with Single Sign-On** button as shown below.
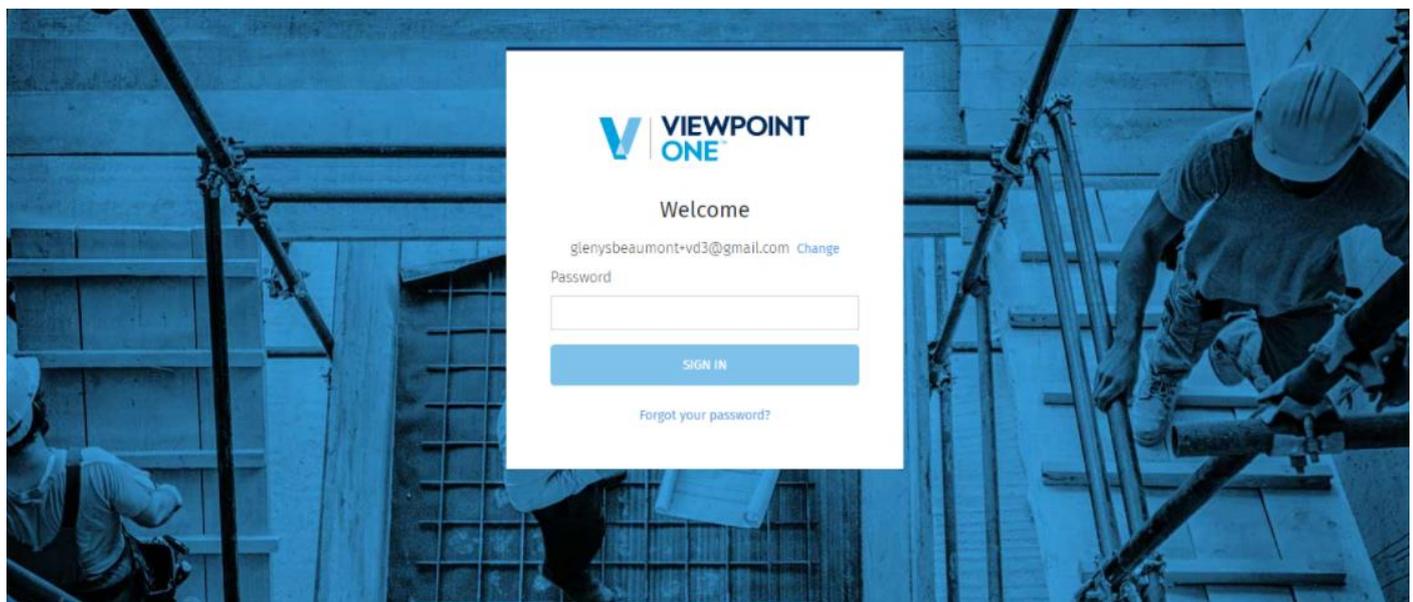

After clicking the **Continue with Single Sign-On** the user will either be redirected to the "ViewpointOne" or "Trimble Construction One" Sign-In page where email address and password is entered (as shown below), or if SSO is activated through Azure AD, or if the user is already signed on with their ViewpointOne ID, then the user will be taken directly into the Jobpac Connect application.

How to change your ViewpointOne ID Password

If a user has transitioned to a ViewpointOne ID they will not be able to change their password in Jobpac Connect and the icon to do that will disappear. With a ViewpointOne ID use the "Forgot your password?" option on the sign-on screen as shown below.

Additional Resources

Tutorial for Azure Active Directory Integration with ViewpointOne

In this tutorial, you learn how to integrate ViewpointOne with Azure Active Directory (Azure AD). Integrating ViewpointOne with Azure AD provides you with the following benefits:

- You can control in Azure AD who has access to ViewpointOne
- You can enable your users to be automatically signed-in to ViewpointOne (Single Sign-On) with their Azure AD accounts.
- You can manage your accounts in one central location - the Azure portal.

If you want to know more details about SaaS app integration with Azure AD, see What is application access and single sign-on with Azure Active Directory. If you don't have an Azure subscription, create a free account before you begin.

Prerequisites

To configure Azure AD integration with ViewpointOne, you need the following items:

- An Azure AD subscription. If you don't have an Azure AD environment, you can get a free account
- ViewpointOne single sign-on enabled subscription

Scenario description

In this tutorial, you configure your ViewpointOne enterprise and configure Azure AD single sign-on for your environment. Note: ViewpointOne leverages the OpenId Connect and OAuth integration with Azure AD. You will first configure your ViewpointOne enterprise to integrate with Azure AD, then add the ViewpointOne enterprise application to your Azure portal instance.

Configure ViewpointOne Single Sign-On

The Viewpoint team will enable your ViewpointOne enterprise to integrate with your Azure Active Directory instance. To configure single sign on for ViewpointOne, contact the Viewpoint Support team and be prepared to provide your target domain name (e.g viewpoint.com) through which you are logging into ViewpointOne.
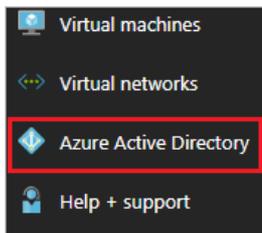
This step must be completed before moving on to adding the ViewpointOne enterprise application to your Azure instance.

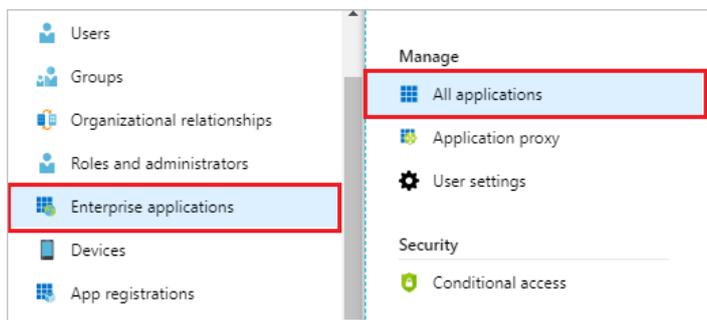### Adding ViewpointOne from the gallery

To configure the integration of ViewpointOne into Azure AD, you need to add ViewpointOne application from the gallery to your list of managed SaaS apps.

To add ViewpointOne from the gallery, perform the following steps:

1. In the Azure portal, on the left navigation panel, click Azure Active Directory icon.
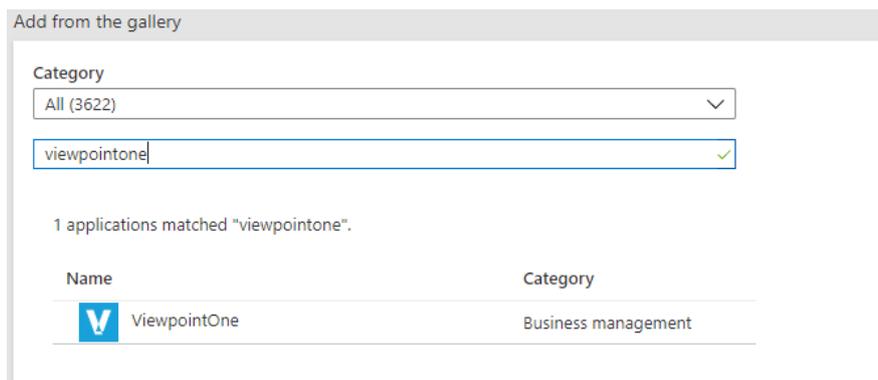

2. Navigate to Enterprise Applications and then select the All Applications option.

3. To add new application, click New application button on the top of dialog.

4. In the search box, type "ViewpointOne", select ViewpointOne from the result panel,
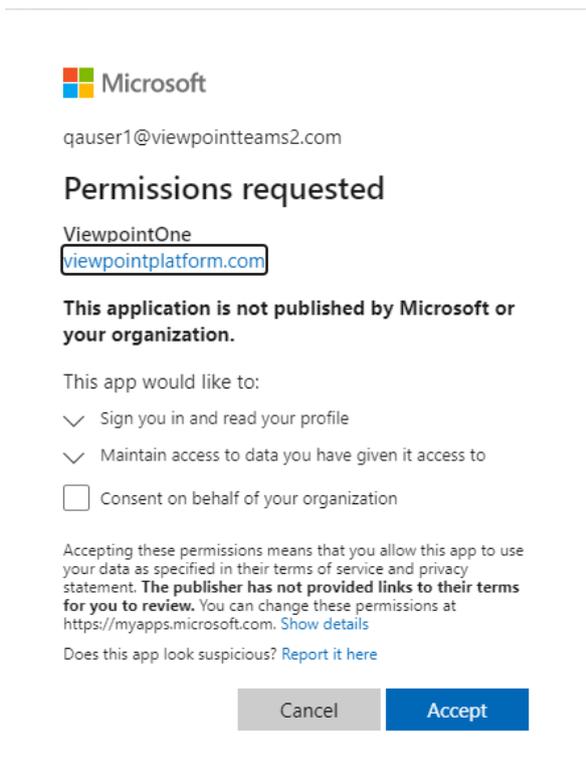

5. Select 'Sign up for ViewpointOne'

Note: For OpenId Connect and OAuth apps, the Add button is disabled by default. Here the tenant admin should select the sign-up button and provide the consent to the application. The application is then added to the customer tenant, where you can do the configurations. There is no need to add the application explicitly.

6. When you select the sign-up link, you are redirected to the ViewpointOne Sign In page for sign-in credentials. Sign in with ViewpointOne enterprise admin credentials.

7. After successful authentication, you accept the consent from the consent page. You can accept consent on behalf of your organization (all users) or each user will have to accept consent. Typically, consent is accepted on behalf of all users. After that, the application home page appears.

After that, the application home page appears.

8. As each user logs in for the first time, they will be prompted for their Microsoft (Azure AD) password. Subsequently, they will be authenticated without having to enter their password.