# Single Sign On (SSO) Identity Providers

Last Modified on 06/18/2025 11:28 am CDT

# Overview

Single Sign On (SSO) allows you to control access to Beyond using your own Identity Provider instead of having users log in with their TempWorks credentials.

This allows you to use your Identity Provider to enforce whatever sign in requirements you see fit, including things like multi-factor authentication, password strength requirements, or requiring the user to be logging in from a certain IP range or corporate network.

Currently, SSO works with Beyond and the Outlook Add-In, and the same settings are applied to both products.

\*Note\* This integration does require initial setup by TempWorks.

For more information about getting this setup, and pricing inquiries, please contact your TempWorks Account Manager.

## **Identity Providers**

An Identity Provider is a service for managing user accounts that your users can log into from another application.

Examples of Identity Providers include:

- Azure AD
- Active Directory Federation Services
- CyberArk
- OKTA
- OneLogin
- SecureAuth

\*Note\* TempWorks does not support SSO through the following:

- Google Cloud Identity & Amazon Web Services (AWS) Single Sign On.
- Personal Google accounts, Facebook, or other social media accounts.

For an Identity Provider to be compatible with SSO, it must utilize the OAuth 2.0 protocol using OpenID Connect.

### **Identity Provider Setup**

While you have the ability to use any major Identity Provider that utilizes the OAuth 2.0 protocol using OpenID Connect (examples above), TempWorks clients have seen immediate success using Azure AD (Active Directory).

The following is a basic setup example within Azure AD.

\*Note\* To access the areas of Azure AD outlined below, you will need to have an account with Azure AD along with administrative permissions within Beyond.

### **Standard Azure AD Example**

Begin by logging into Azure AD (Active Directory):



From the landing page, navigate to "App Registrations" within the left sidebar:

=	Microsoft Azure			ces, services, and d	ocs (G+/)	
Hor	Home >					
0	Tempworks Software   Overview ···     Azure Active Directory					
-	×	$+$ Add $\vee$ 🔅	Manage tenants [ What's new 🔄 Pr	review features	🖗 Got feedback?	$\checkmark$
U	Overview	0	situation Descention Tatasials			
**	Preview features	Overview	nitoring Properties Lutoriais			
×	Diagnose and solve problems	Search your	tenant			
Mar	nage	Desis in fermation				
2	Users	Basic Information				
24	Groups	Name	Tempworks Software		Users	
ŵ	External Identities	Tenant ID		D	Groups	
2.	Roles and administrators	Primary domain			Applications	
8	Administrative units	,				
щ	Enterprise applications	License			Devices	
q	Devices	Alerts	6			
Ш,	App registrations					
۵	Identity Governance	Upcom	ing TLS 1.0, 1.1 and 3DES deprecation			
8	Application proxy	Please e clients(a	enable support for TLS 1.2 on applications/platform) to avoid any service			
	Custom security attributes (Preview)	impact. Learn m	nore 🖾			

Select "New Registration" and create a registration for "TempWorks Beyond" or whatever name you would like that would be easy to remember:

	Microsoft Azure	∠ Search resources, services, and docs (G+/)
Hom	ne > Tempworks Software	
	Tempworks Soft Azure Active Directory	ware   App registrations 🛷 …
0	Overview	Kefresh 🖞 Download 🔂 Preview features   R Got feedback?
**	Preview features	Starting lung 20th 2020 we will be langer add any new features to Anyze Active Directory Authentication Library (ADAL) and Anyze AD Graph May
×	Diagnose and solve problems	The set of the set
Man	age	
2	Users	All applications Owned applications Deleted applications
24	Groups	
0	External Identities	
2.	Roles and administrators	1 applications found
	Administrative units	Display name To b
щ, і	Enterprise applications	
Щ.	Enterprise applications	

\*Note\* Once you have created the registration of "TempWorks Beyond" or whatever name you would like that would be easy to remember, the following will be automatically generated:

- Directory (Tenant) ID
- Application (Client) ID

Save the above items as they will be needed during the setup of SSO within Beyond.

	✓ Search resources, services, and docs (G+/)
Home > Tempworks Software >	
TempWorks Beyond	\$ <sup>2</sup> ····
✓ Search (Ctrl+/) «	📋 Delete 🜐 Endpoints 🐱 Preview features
R Overview	floor Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). $ o$
Quickstart	
🚀 Integration assistant	∧ Essentials
Manage	Display name : TempWorks Beyond
Branding & properties	Application (client) ID :
Authentication	Object ID :
📍 Certificates & secrets	Directory (tenant) ID : Supported account types : <u>My organization only</u>

While within the "TempWorks Beyond" registration, select "Certificates and Secrets" in the left sidebar:

		✓ Search resources, services, and docs (G+/)
Home > Tempworks Software >		
TempWorks Beyond	\$	
	🗎 Delete 🌐 Endpoints	E Preview features
Noverview	Got a second? We would	love your feedback on Microsoft identity platform (previously Azure AD for developer). $ ightarrow$
ickstart		
🚀 Integration assistant	∧ Essentials	
Manage	Display name	: TempWorks Beyond
🚍 Branding & properties	Application (client) ID	:
Authentication	Object ID	:
	Directory (tenant) ID	:
7 Certificates & secrets	Supported account types	: My organization only

Select "New Client Secret" within the "Client Secrets" tab:

	Microsoft Azure		𝒫 Search resources,	services, and docs (G+	ſ)	
Н	ome > Tempworks Software > TempWo	rks Beyond				
🔶 TempWorks Beyond   Certificates & secrets 🖉 🐇						
8	Search (Ctrl+/) «					
10	Overview	Credentials enable confidential applications to i	dentify themselves to th	e authentication servi	e when receiving tokens at a web addressable location (using an HTTPS	
<b>6</b> 2	Quickstart	scheme). For a higher level of assurance, we reco	ommend using a certific	ate (instead of a client	secret) as a credential.	
*	Integration assistant					
M	anage	<ul> <li>Application registration certificates, secrets a</li> </ul>	and federated credentials	can be found in the tab	s below.	×
	Branding & properties					
Э	Authentication	Certificates (0) Client secrets (2) Fed	derated credentials (0)			
Ť	Certificates & secrets	A secret string that the application uses to pro-	we its identity when req	uesting a token. Also o	an be referred to as application password.	
10	Token configuration	L Marine Brank annual				
->	API permissions	T New client secret				
	Expose an API	Description	Expires	Value ()	Secret ID	
	App roles					
20	Owners					

Enter the following information:

- Description: Enter a description for the Client Secret.
- Expires: Cannot be longer than 24 months when selecting "custom".

\*Note\* The expiration date cannot be longer than 24 months when selecting "custom".

\*Warning\* A new Client Secret will need to be created and added within Beyond before the expiration date of the original. If this is not done, users will be unable to log into Beyond once the original Client Secret expires.

Add a client secret		
Description	Enter a description for this client secret	
Expires	Recommended: 6 months	$\sim$

Select "Add"

\*Note\* Copy the "Client Secret" immediately after creating it to be added to Beyond.

Navigating away and back to this screen will hide the "Client Secret", making it unable to be copied, resulting in a new Client Secret needing to be created.

	2	Search resources, search re	ervices, and docs (G+/)			
Home > Tempworks Software > TempW	orks Beyond					
🔶 TempWorks Beyond   Certificates & secrets 🛛 🖈 👘						
Search (Ctrl+/) «	R Got feedback?					
Overview						
🍊 Quickstart	$\bigcirc$ Got a second to give us some feedback? $\rightarrow$					×
🚀 Integration assistant						
Manage	Credentials enable confidential applications to ider scheme). For a higher level of assurance, we recom	ntify themselves to the mend using a certifica	authentication service whe te (instead of a client secre	en receiving tokens at t) as a credential.	a web addressable location (using an HTTP	5
Branding & properties						
Authentication	Application registration certificates, secrets and	l federated credentials c	an be found in the tabs below	v.		×
📍 Certificates & secrets						
Token configuration	Certificates (0) Client secrets (3) Feder	ated credentials (0)				
- API permissions	A secret string that the application uses to prove	its identity when requ	esting a token. Also can be	referred to as applica	tion password.	
Expose an API		,				
App roles	+ New client secret					
A Owners	Description	Expires	Value 🛈		Secret ID	
🤱 Roles and administrators	Login Server SSO PoC	7/14/2022				
Manifest	New Beyond Secret	11/25/2022		Ð		
Support + Troubleshooting	Beyond Client Secret	12/31/2299				

While within the "TempWorks Beyond" registration, select "Authentication" in the left sidebar:

≡ Microsoft Azure	𝒫 Search resources, services, and docs (G+/)
Home > Tempworks Software > TempW	forks Beyond
💡 TempWorks Beyond	Certificates & secrets 👒 …
Search (Ctrl+/) «	₽ Got feedback?
Overview	Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressal
🍊 Quickstart	scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.
🚀 Integration assistant	
Manage	Application registration certificates, secrets and federated credentials can be found in the tabs below.
Branding & properties	
Authentication     m     Authentication     m	Certificates (0) Client secrets (2) Federated credentials (0)
Certificates & secrets	A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Navigate to Beyond > B Menu > System Settings > Security > Authentication > Single Sign On > Redirect URL > More Details > Copy:

\*Note\* The "Redirect URL" will be custom to your company and will be configured during the initial setup by TempWorks.

<b>B</b> 🕹 🗈 💻		
Settings > System Settings >	Security > Authentication	
System Settings	Authentication	
Advanced Search	Authentication methods defined will be applied to the entire organization.	
Content	Single Sign On	
External Service	Status	
Insight Widgets	Redirect URL ⑦	
Job Board		
On-Site Time Clock Invite Co	FEWER DETAILS	
Organization	EDIT DEACTIVATE	

Navigate back to Azure AD > Authentication > Web > Redirect URI's > Add URI:

	∠ Search resources, services, and docs (G+/)	
Home > Tempworks Software > TempWo	orks Beyond	
→ TempWorks Beyond	Authentication 🖈 …	
•		
Search (Ctrl+/) «	R Got feedback?	
Overview	∧ Web Quickstart Docs [7]	Ŵ
Quickstart	Redirect URIs	
🚀 Integration assistant	The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI ye 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 of the second sec	ou
Manage		1
🚍 Branding & properties		Î
Authentication		Î
📍 Certificates & secrets		Î
Token configuration		<u>ل</u>
API permissions		<u>ل</u>
Expose an API		<u>ت</u>
App roles		<u>一</u>
A Owners		. UU
2 Roles and administrators		
Manifest		
Support + Troubleshooting		
P Troubleshooting	Ν	■
New support request	1-2-	<u>اللا</u>
-		
		回 曲
	Add URI	

Paste the "Redirect URL" into the "Add URI" section.

Check the box for "ID Tokens" within the "Implicit grant and hybrid flows" section:

	✓ Search resources, services, and docs (G+/)				
Home > Tempworks Software > TempWorks Beyond					
TempWorks Beyond   Authentication * ···					
Search (Ctrl+/) «	₽ Got feedback?				
R Overview	Implicit grant and hybrid flows				
🍊 Quickstart	Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and				
🚀 Integration assistant	doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID toke For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more abr				
Manage	tokens.				
Branding & properties	Select the tokens you would like to be issued by the authorization endpoint:				
Authentication	D tokens (used for implicit nows)				
📍 Certificates & secrets					
Token configuration	Supported account types				
-> API permissions	Who can use this application or access this API?				
Expose an API	<ul> <li>Accounts in this organizational directory only (Tempworks Software only - Single tenant)</li> </ul>				
App roles	Accounts in any organizational directory (Any Azure AD directory - Multitenant)				
A Owners	Help me decide				

Select the option for "Accounts in this organizational directory only" within the "Supported account types" section:

≡ Microsoft Azure	, ✓ Search resources, services, and docs (G+/)			
Home > Tempworks Software > TempWorks Beyond TempWorks Beyond   Authentication * ···				
Search (Ctrl+/) «	R Got feedback?			
<ul> <li>Werview</li> <li>Quickstart</li> <li>Integration assistant</li> <li>Manage</li> </ul>	Implicit grant and hybrid flows Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.			
🗧 Branding & properties	Select the tokens you would like to be issued by the authorization endpoint:			
Authentication	Access tokens (used for implicit flows)			
📍 Certificates & secrets				
Token configuration	Supported account types			
-> API permissions	Who can use this application or access this API?			
Expose an API	Accounts in this organizational directory only (Tempworks Software only - Single tenant)			
App roles	Accounts in any organizational directory (Any Azure AD directory - Multitenant)			
A Owners	Help me decide			

Select "No" for "Enable the following mobile and desktop flows" within the "Advanced settings" section:



Select "Save" to save all the changes that have been applied:



Once the Identity Provider setup is complete, you are ready to add the following information into Beyond and complete the setup of SSO:

1. Identity Provider URL: "https://login.microsoftonline.com/{YourAzureTenantId}" with the

[YourAzureTenantID] being the "Directory (Tenant) ID" from Azure AD.

- 2. Client ID: This is the "Application (Client) ID" from Azure AD.
- 3. Client Secret: This is the "Client Secret" from Azure AD.
- 4. Claim Name: This is "upn" for setups using Azure AD.

### **Active Directory Federation Services Example**

\*Note\* The following setup process assumes you have the Federation Services role installed and configured to use OpenID Connect.

Begin by opening the Active Directory Federation Services (ADFS) Management MMC snap-in and navigate to the "Application Group":



Select "Add Application Group" on the right and within the "Add Application Group Wizard", enter/select the following:

- Name: Enter the name of the Application Group.
- Description: Enter the description of the Application Group.
- Template: Select the "Server Application" template.

🍓 Add Application Group Wizard × Welcome Steps Name: Welcome Tempworks - SSO - Production Server application Description: Configure Application Ability for Tempworks Beyond to authenticate with ADFS as an external identity provider using OpenID Credentials Connect Summarv Complete Template: **Client-Server applications** Native application accessing a web API Server application accessing a web API Web browser accessing a web application Standalone applications Native application Server application Web API

Select "Next" to add the application. Update the "Name" and/or "Client Id" as needed, but the generated GUID identifier can be used without issue:

\*Note\* During this step, you can add a placeholder "Redirect URL". This will be changed to the appropriate URL once the information is being added to Beyond at a later step.

翰 Add Application Group Wizard

Server application		
Steps	Name:	
Welcome	Tempworks - SSO - Production - Server application 1	
Server application	Client Identifier:	
<ul> <li>Configure Application Credentials</li> </ul>		
Summary	Redirect URI:	
Complete	https://temporaryUrl.com	Add
		Remove
	Description:	1
		]
	< Previous Next >	Cancel

Select "Next" to proceed to the "Configure Application Credentials" step.

Add application credentials by selecting the "Generate a Shared Secret" option:

Steps	Select credentials used by the application to authenticate itself with AD FS when requesting	access tokens.
Welcome     Server application     Configure Application	Register a key used to sign JSON Web Tokens for authentication     Configure	
Credentials Summary Complete	Windows Integrated Authentication Select the AD Account: Example: CONTOSO\expensevc	Select
	Generate a shared secret	00000
		Copy to clipboard
	Copy and save the secret. You will not be able to view the secret after the app created. You can reset the secret later if required	plication group is

\*Note\* Save the Secret somewhere safe as it will no longer be visible after finishing this step.

 $\times$ 

If the Secret is lost/forgotten, it can be reset later.

Navigate to Beyond > B menu > System Settings > Security > Authentication > Methods > Edit the Single Sign-On method that was added by TempWorks Support.

\*Note\* Active Directory Federation Services (ADFS) will need to be publicly accessible.

Within the "Edit SSO" window, enter/select the following:

• Identity Provider URL: The Base URL for the OpenID Connect (OIDC) metadata endpoint.

\*Note\* Navigate to the metadata endpoint in your web browser and get the JSON output for ADFS OIDC metadata. The metadata URL is your Base URL.

- Client ID: The "Client Identifier" from the ADFS setup process.
- Client Secret: The "Shared Secret" from the ADFS setup process.
- Claim Name: Enter "unique\_name".
- Use Claim to Look Up User By: Select "External User Identifier".

\*Note\* For this setup example, we are going to use our domain username to map identity to our Tempworks Service Rep Record. ADFS puts the domain username in as the "unique\_name" claim (in the format of <domain>\<username>).

The "Use Claim to Look Up User By" option should then use "External User Identifier".

In the service rep settings for each user, the user's domain username will need to be added to the "External User Identifier" field within B Menu > System Settings > Service Representatives.

• Active: Checked

Settings / 🔤	/ Methods	
	Methods	Edit SSO 🕲
	Authentication methods defined will	* Identity Provider URL https://
ies	Single Sign On	* Client Id
/Janagement	Status	Client Secret
tions	Redirect URL (2)	Claim Name
nent Types	EDIT DEACTIVATE	If not specified, "sub" will be used
		Use Claim to look up user by: O TempWorks Username
מו		External User Identifier
211		
		i Only new sessions will be affected by the applied authentication method. Existing sessions will not be affected.
		CANCEL SUBMIT

Select "Submit" to finalize the changes.

Back within the "Authentication Methods" card, select the "Copy" icon to copy the "Redirect URL":

Methods				
Authentication methods defined will be applied to the entire organization.				
Single Sign On				
Status	Active			
Redirect URL 🍘	https://login.onte mpworks.com/acc ount/external/sig nin- oidc/			
EDIT DEACTIVATE				

Navigate back to the ADFS Management UI and within the "Application Groups", navigate to the "Properties" of the Application Group you had previously created. Select "Edit" and replace the placeholder "Redirect URL" with

#### the URL generated from Beyond:

🙀 AD FS			
🗌 File Action View Window Help	)		
AD FS	Application	Groups	Actions
Service	Tempworks - SSO	- Production Properties X	Application Grou
Authentication Methods	Ganaral		Add Applicat
Certificates	General		View
Claim Descriptions	Name:		New Windov
Device Registration     Endpoints	Tempworks - SS	O - Production	
Scope Descriptions	Description:	Tempworks - SSO - Production - Server application Properties	×
Web Application Proxy	Ability for Tempy	General Confidential	
Access Control Policies		Nama	
Claims Provider Trusts		Tempworks - SSO - Production - Server application	
Application Groups	Applications:		
	Name	Client Id:	
	Server applie		
	Tempworks - S	Redirect URI:	
			Add
		https://login.ontempworks.com/account/external/signin-oidc/	Remove
		< >	
		Description.	

\*Note\* It is recommended to restart the "Active Directory Federation Services" service on each server in your ADFS farm to ensure they are all using the new config.

Back within Beyond, after selecting the "Sign In With SSO" button on the bottom of the login screen another screen is presented that asks for an email or domain. Enter in the domain host name associated with the ADFS integration:



Sign in v	vith SSO	
Company e	email or domain .com	-
	SIGN IN	
	Back	
	build 5.2025.417.1 - production	

After selecting "Sign In", it will redirect the browser out to the company's ADFS sign in page to complete the domain credential sign in. This will then redirect back to the Beyond sign-in process once complete.

\*Note\* You may not see this step if you have previously signed into the company ADFS login page and still have an active cookie session.

### **Related Articles**