Single Sign On (SSO) Identity Providers

Last Modified on 08/02/2023 3:01 pm 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.

This article covers the following:

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

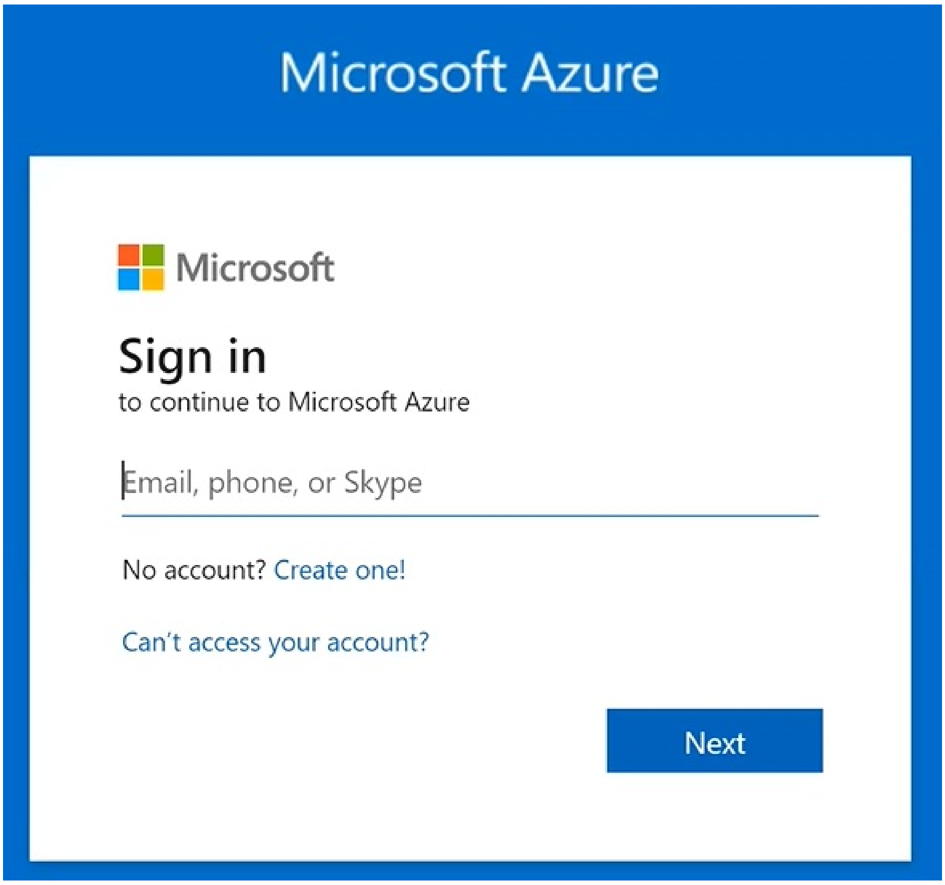
While you have the ability to use any major Identity Provider that utilizes the OAuth 2.0 protocol using OpenID Connect (examples above), TempWorks clients have seen immediate success using Azure AD (Active Directory).

The following is a basic setup example within Azure AD.

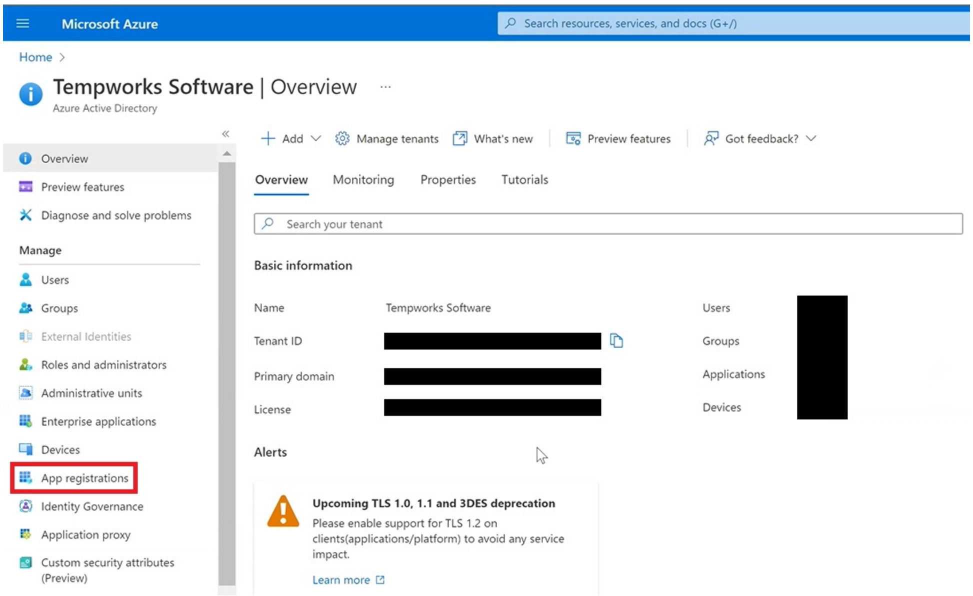
Note To access the areas of Azure AD outlined below, you will need to have an account with Azure AD along with administrative permissions within Beyond.

Standard Azure AD Example

Begin by logging into Azure AD (Active Directory):



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



Name Tempworks Software

Tenant ID [redacted]

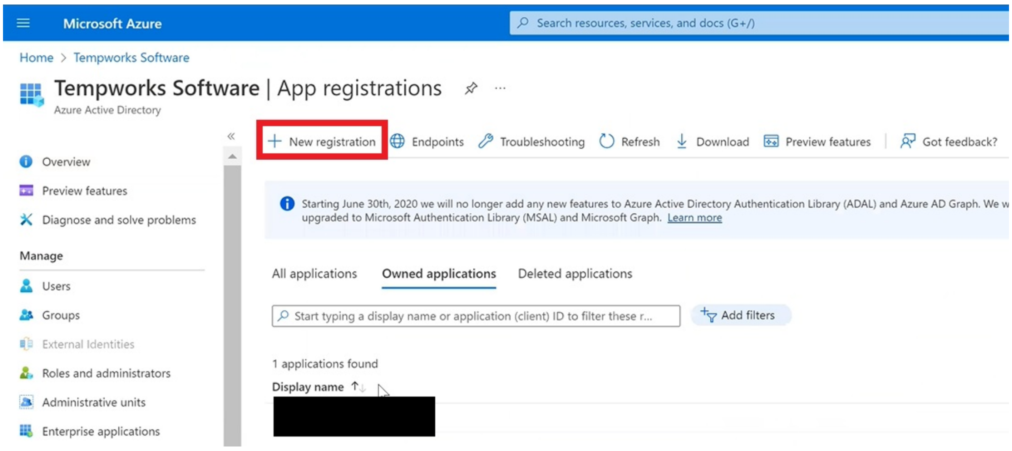
Primary domain [redacted]

License [redacted]

Users
Groups
Applications
Devices [redacted]

Upcoming TLS 1.0, 1.1 and 3DES deprecation
Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.

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



Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We w upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

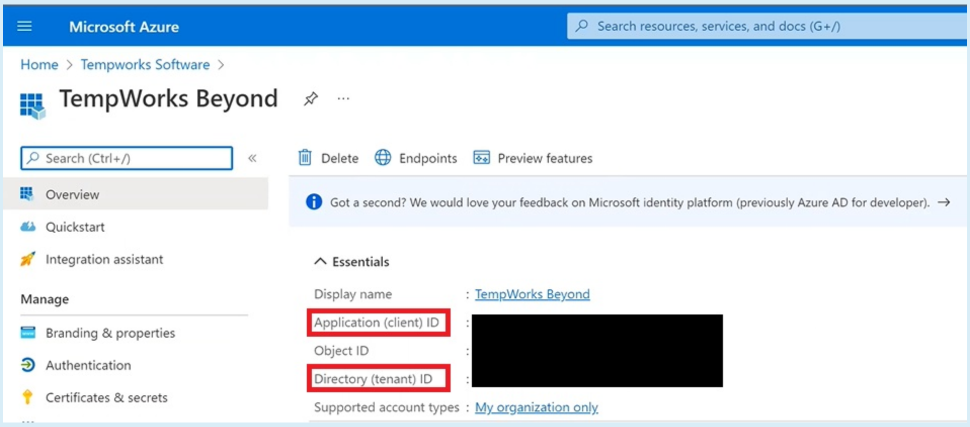
1 applications found

[redacted]

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

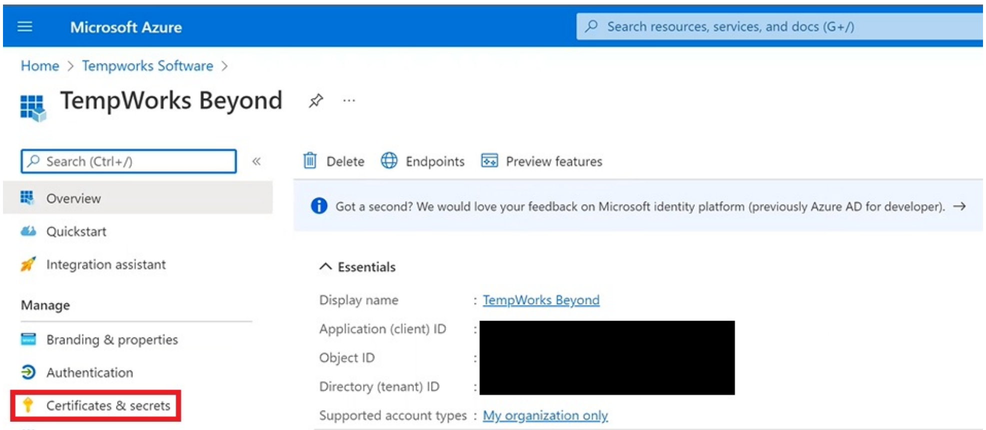
Save the above items as they will be needed during the setup of SSO within Beyond.



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

Display name : TempWorks Beyond
Application (client) ID :
Object ID :
Directory (tenant) ID :
[redacted]
Supported account types : My organization only

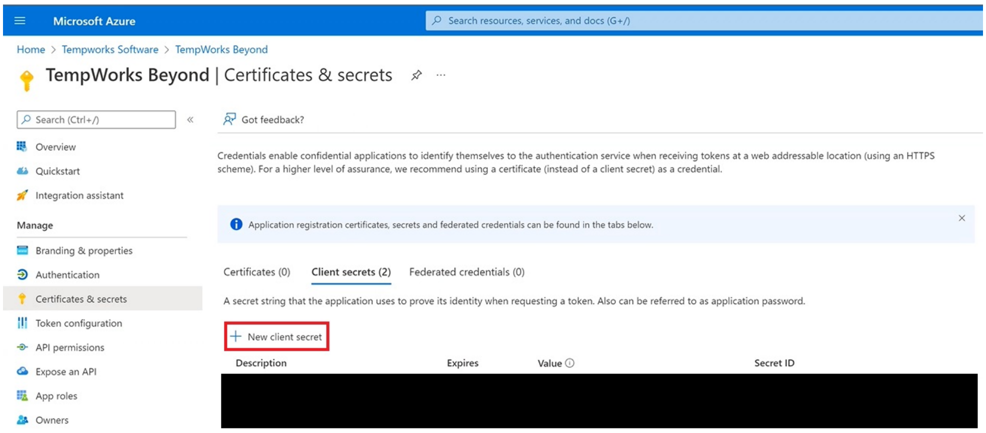
While within the "TempWorks Beyond" registration, select "Certificates and Secrets" in the left sidebar:



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

Display name : TempWorks Beyond
Application (client) ID :
Object ID :
Directory (tenant) ID :
[redacted]
Supported account types : My organization only

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



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Tempworks Software > TempWorks Beyond

TempWorks Beyond | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value ⓘ	Secret ID

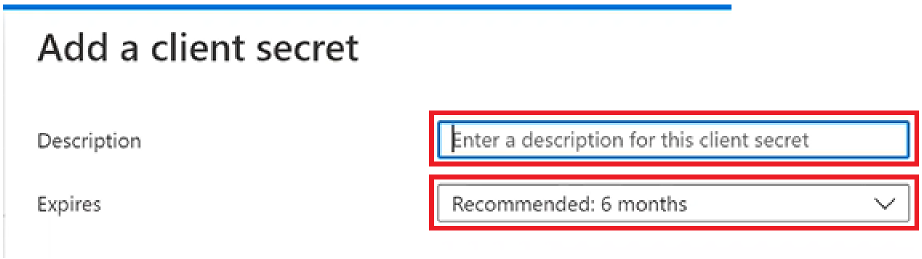
[redacted]

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

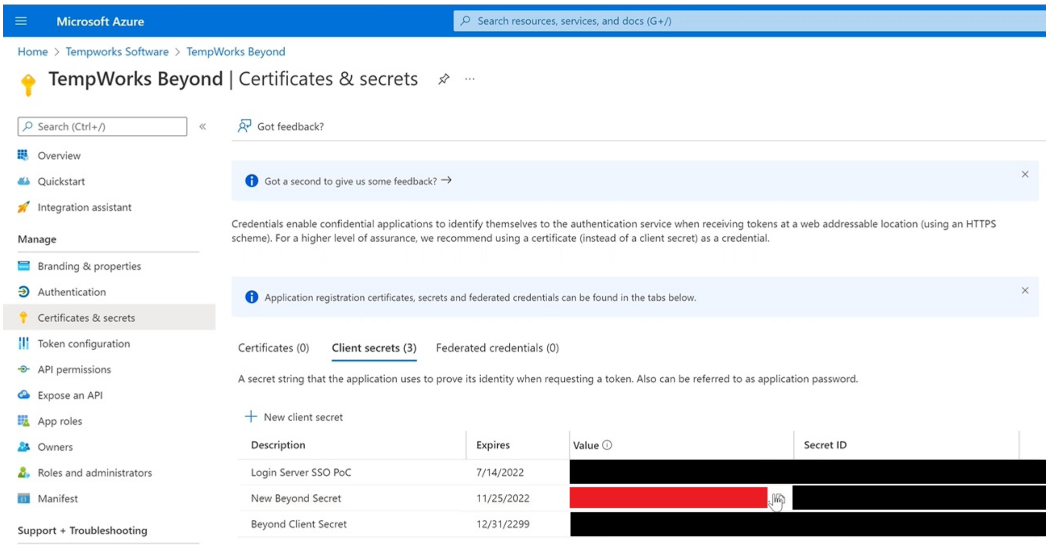
Description: Enter a description for this client secret

Expires: Recommended: 6 months

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.



Got a second to give us some feedback? →

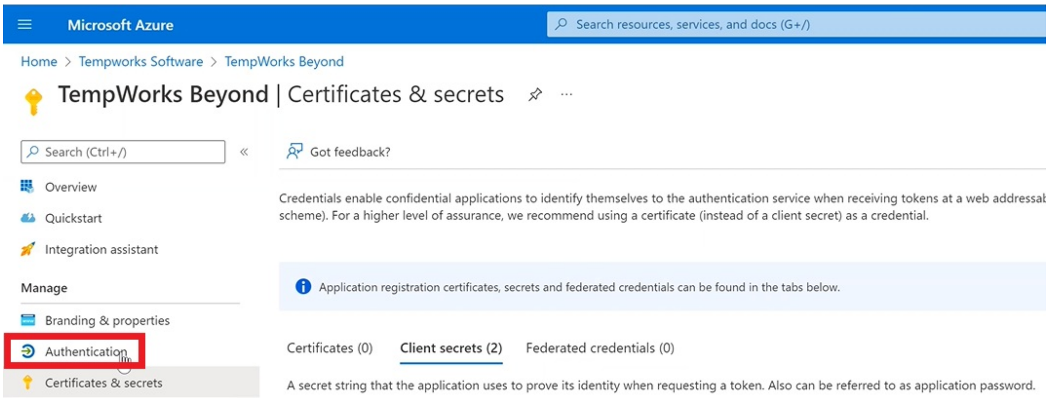
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
Login Server SSO PoC	7/14/2022	[redacted]	[redacted]
New Beyond Secret	11/25/2022	[redacted]	[redacted]
Beyond Client Secret	12/31/2299	[redacted]	[redacted]

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



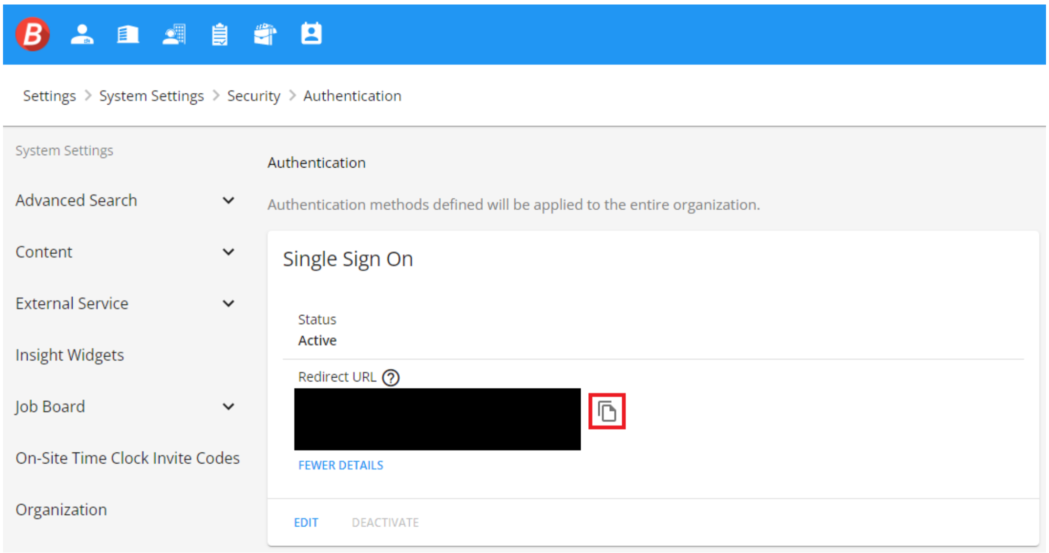
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressat scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

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.



Authentication

Authentication methods defined will be applied to the entire organization.

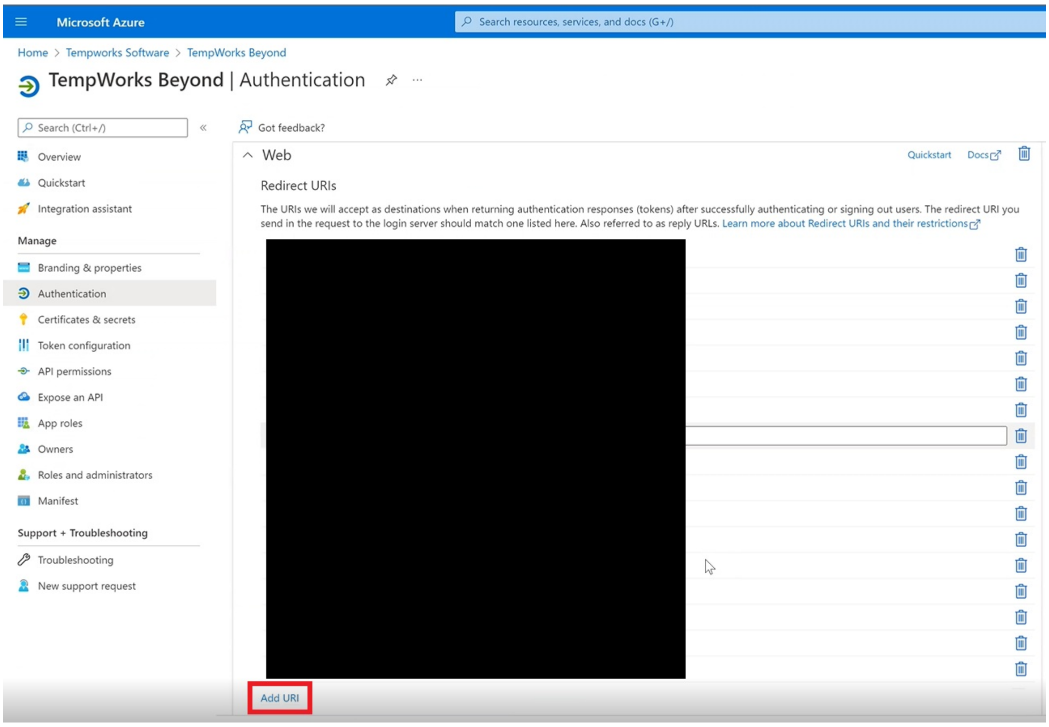
Single Sign On

Status
Active

Redirect URL

[redacted]

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



TempWorks Beyond | Authentication

Web

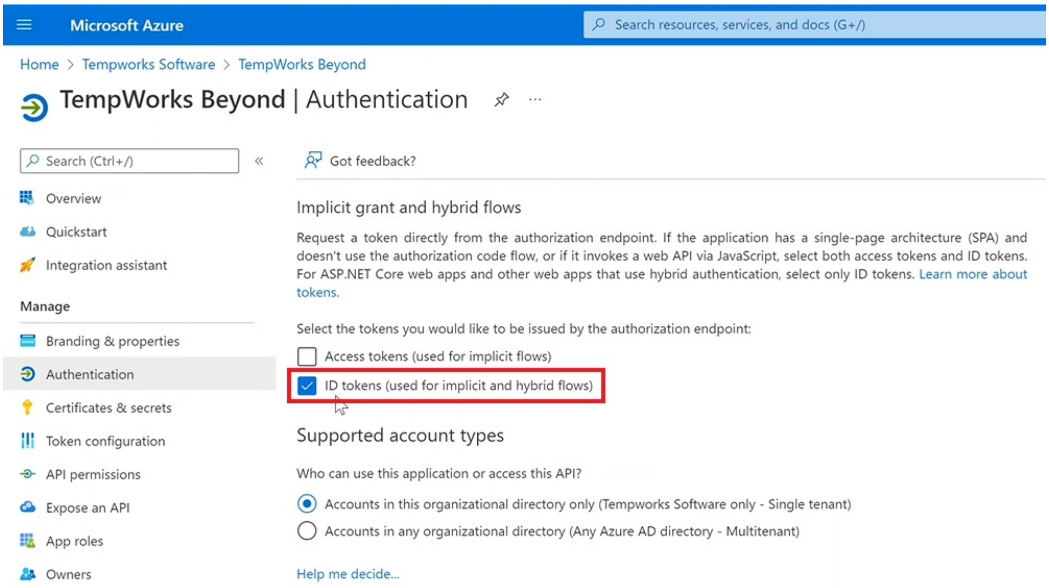
Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out 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

[redacted]

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

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



Home > Tempworks Software > TempWorks Beyond

TempWorks Beyond | Authentication

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.

Select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens (used for implicit flows)

☑ ID tokens (used for implicit and hybrid flows)

Supported account types

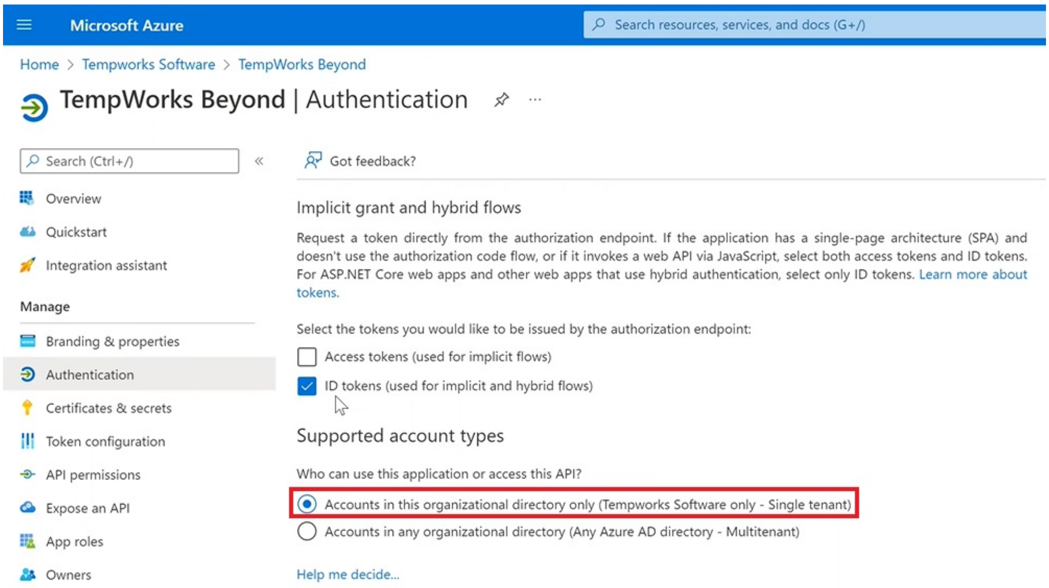
Who can use this application or access this API?

● Accounts in this organizational directory only (Tempworks Software only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

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



Home > Tempworks Software > TempWorks Beyond

TempWorks Beyond | Authentication

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.

Select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens (used for implicit flows)

☑ ID tokens (used for implicit and hybrid flows)

Supported account types

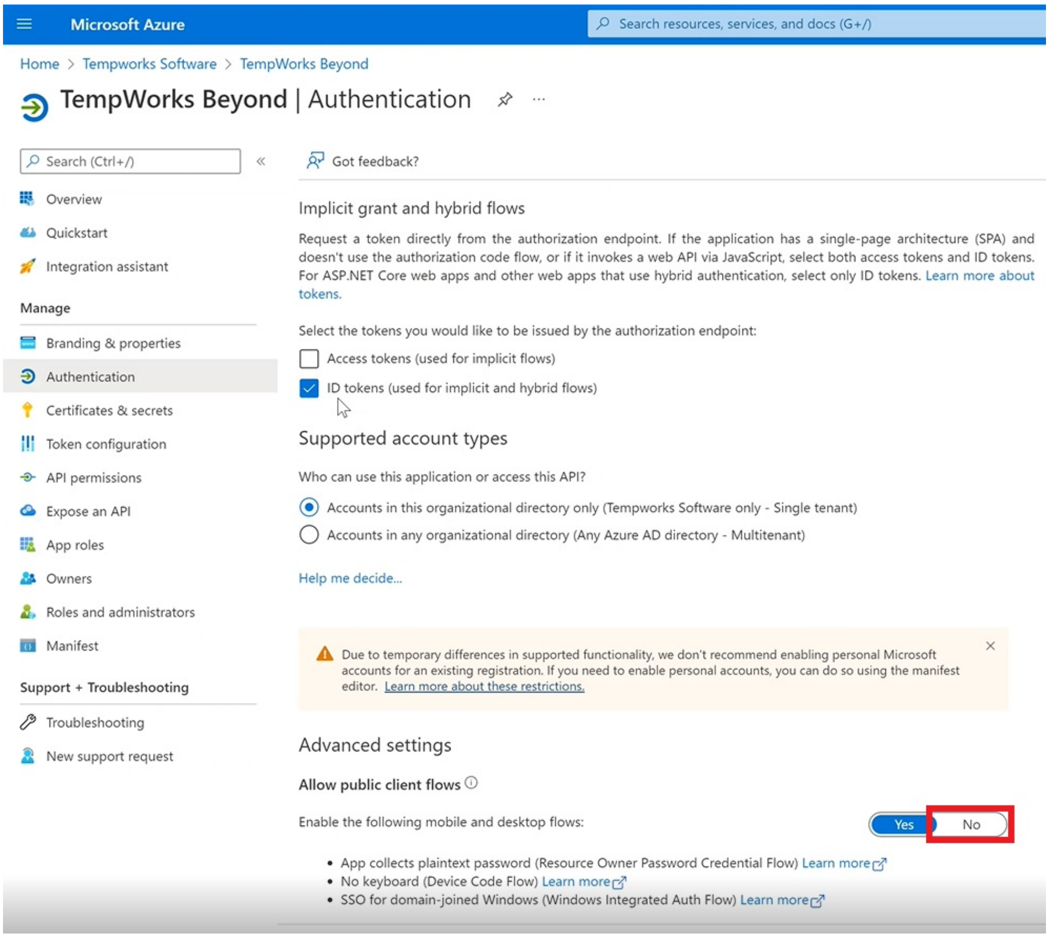
Who can use this application or access this API?

● Accounts in this organizational directory only (Tempworks Software only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

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



TempWorks Beyond | Authentication

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.

Select the tokens you would like to be issued by the authorization endpoint:

□ Access tokens (used for implicit flows)

☑ ID tokens (used for implicit and hybrid flows)

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Tempworks Software only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

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.

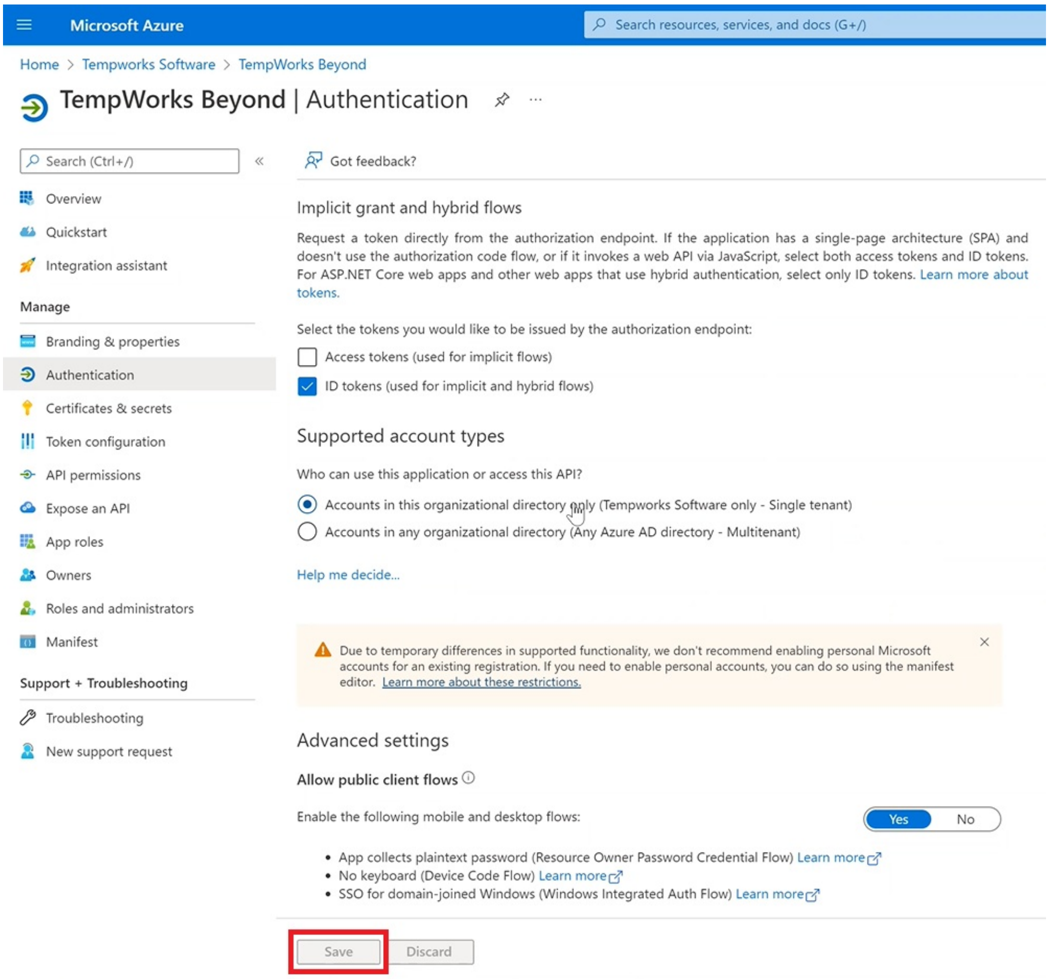
Advanced settings

Allow public client flows

Enable the following mobile and desktop flows: Yes [✓ No]

- App collects plaintext password (Resource Owner Password Credential Flow) Learn more
- No keyboard (Device Code Flow) Learn more
- SSO for domain-joined Windows (Windows Integrated Auth Flow) Learn more

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



TempWorks Beyond | Authentication

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.

Select the tokens you would like to be issued by the authorization endpoint:

□ Access tokens (used for implicit flows)

☑ ID tokens (used for implicit and hybrid flows)

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Tempworks Software only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

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

Allow public client flows

Enable the following mobile and desktop flows: [✓ Yes] No

- App collects plaintext password (Resource Owner Password Credential Flow) Learn more
- No keyboard (Device Code Flow) Learn more
- SSO for domain-joined Windows (Windows Integrated Auth Flow) Learn more

Next Steps

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.

> *Note* To complete the SSO setup process in Beyond, please see the following article titled Beyond - Single Sign-On.

Related Articles