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).

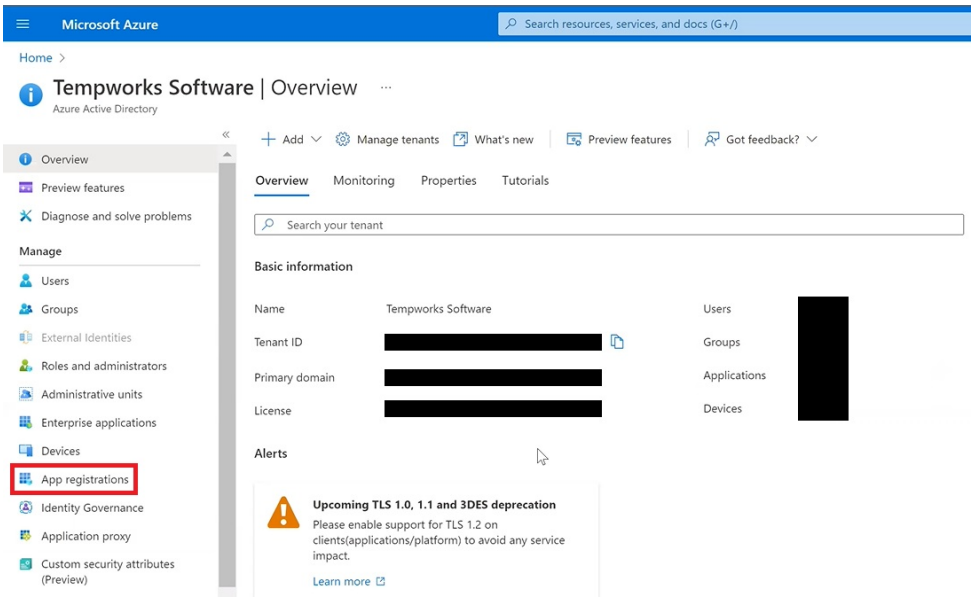
The following is a basic setup example within Azure AD.

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.

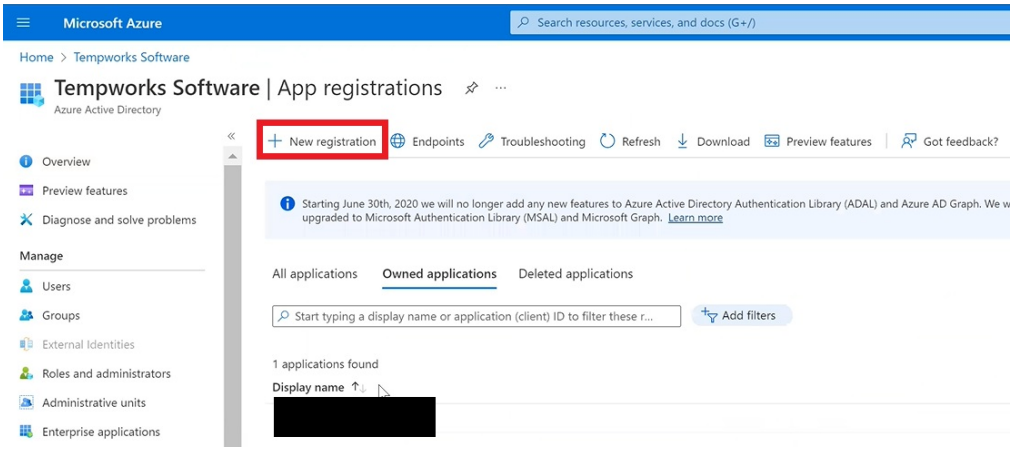
Standard Azure AD Example

Begin by logging into Azure AD (Active Directory):

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



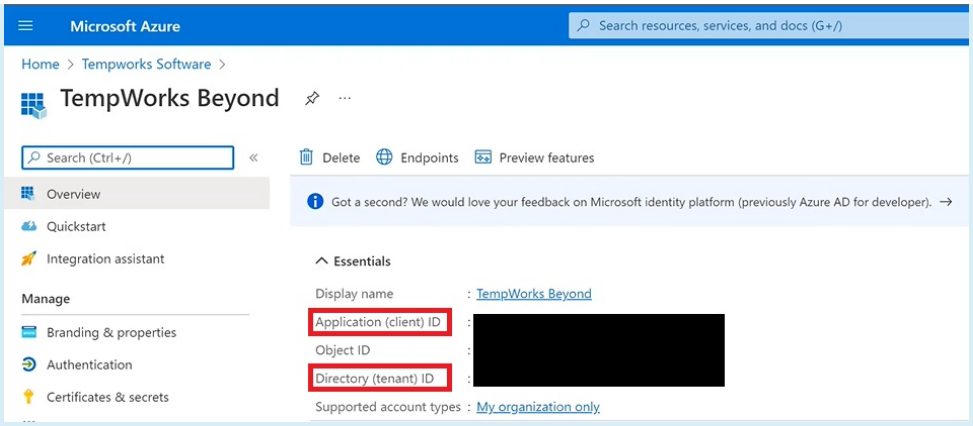
Select "New Registration" and create a registration for "TempWorks Beyond" or whatever name you would like that would be easy to remember:



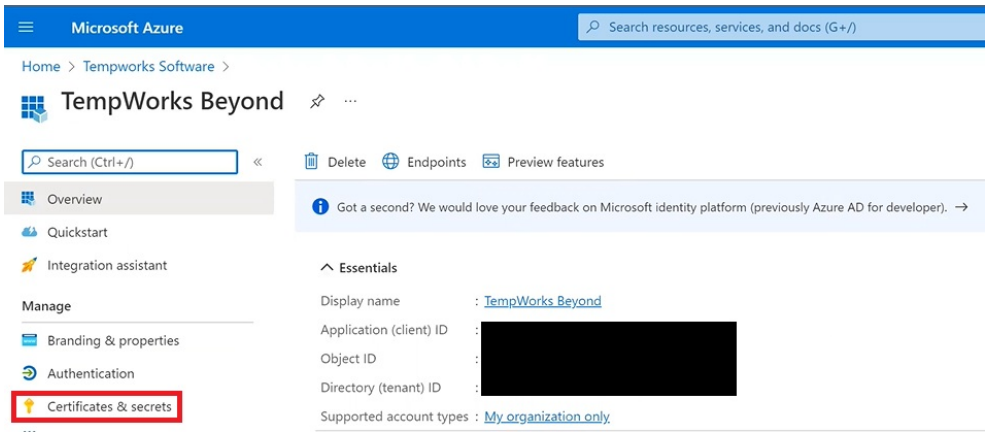
Note Once you have created the registration of "TempWorks Beyond" or whatever name you would like that would be easy to remember, the following will be automatically generated:

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

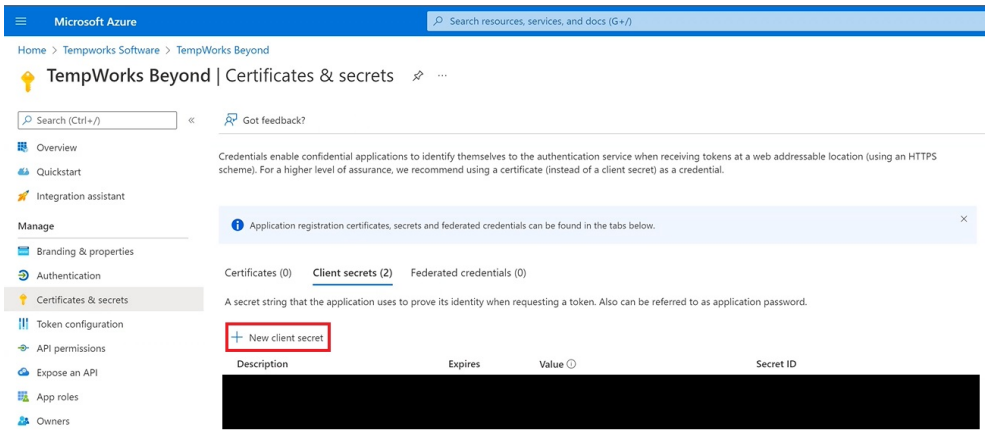
Save the above items as they will be needed during the setup of SSO within Beyond.



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



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

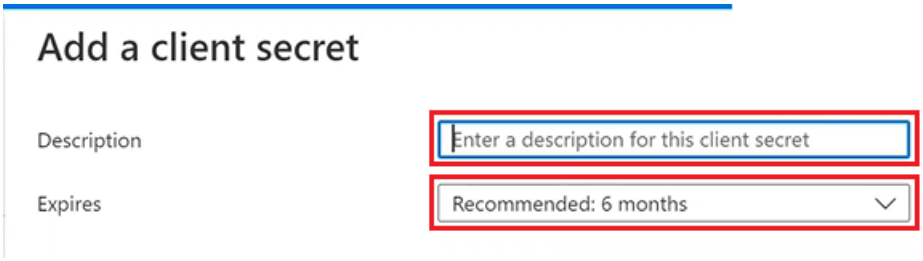


Enter the following information:

- 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".

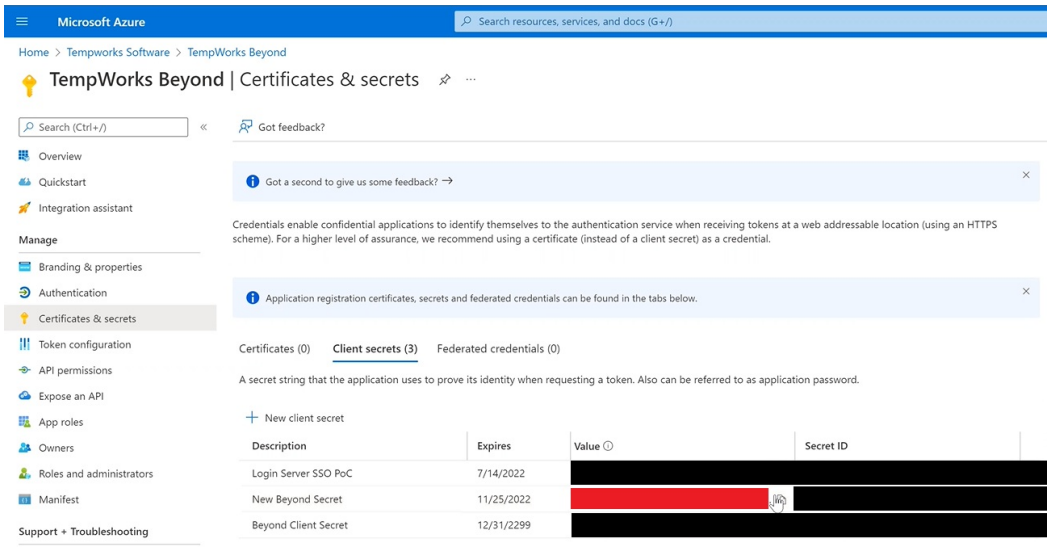
Warning A new Client Secret will need to be created and added within Beyond before the expiration date of the original. If this is not done, users will be unable to log into Beyond once the original Client Secret expires.



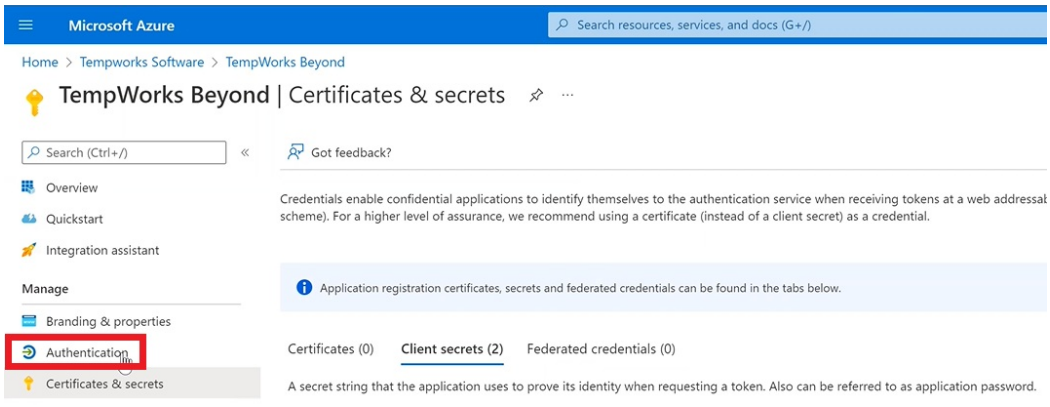
Select "Add"

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.

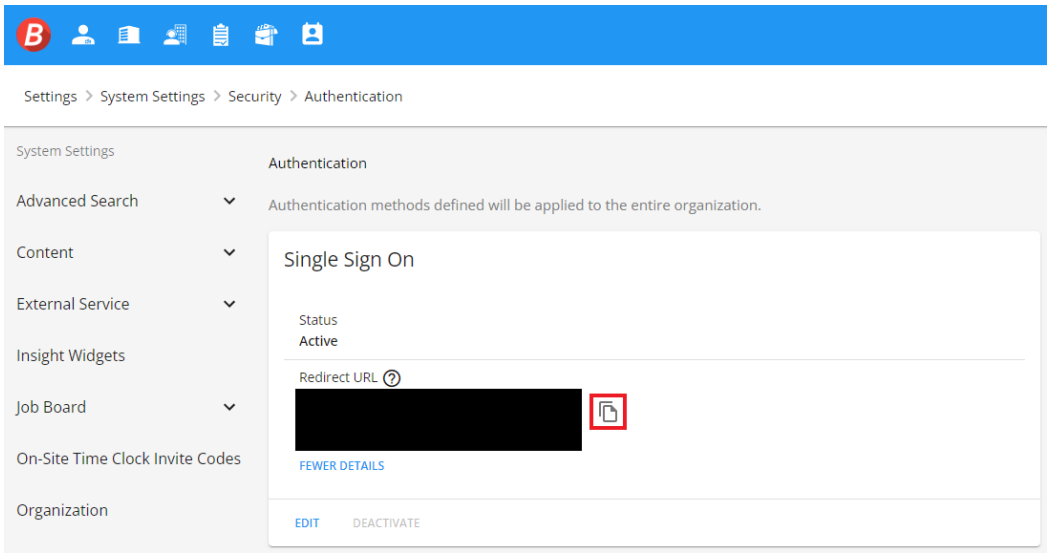


While within the "TempWorks Beyond" registration, select "Authentication" in the left sidebar:

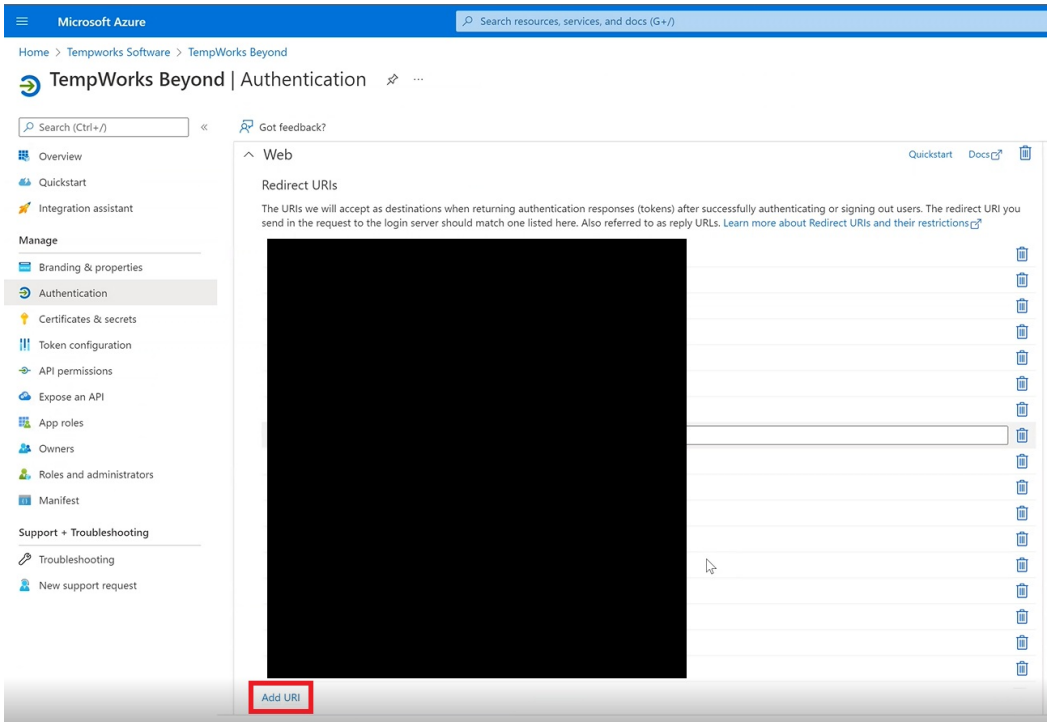


Navigate to Beyond > B Menu > System Settings > Security > Authentication > Single Sign On > Redirect URL > More Details > Copy:

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

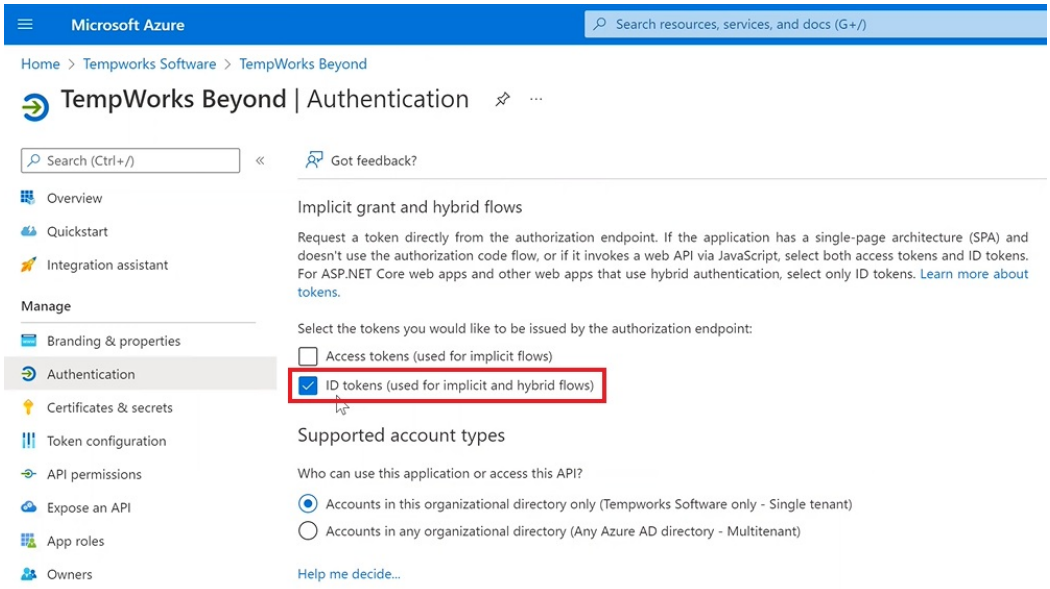


Navigate back to Azure AD > Authentication > Web > Redirect URI's > Add URI:

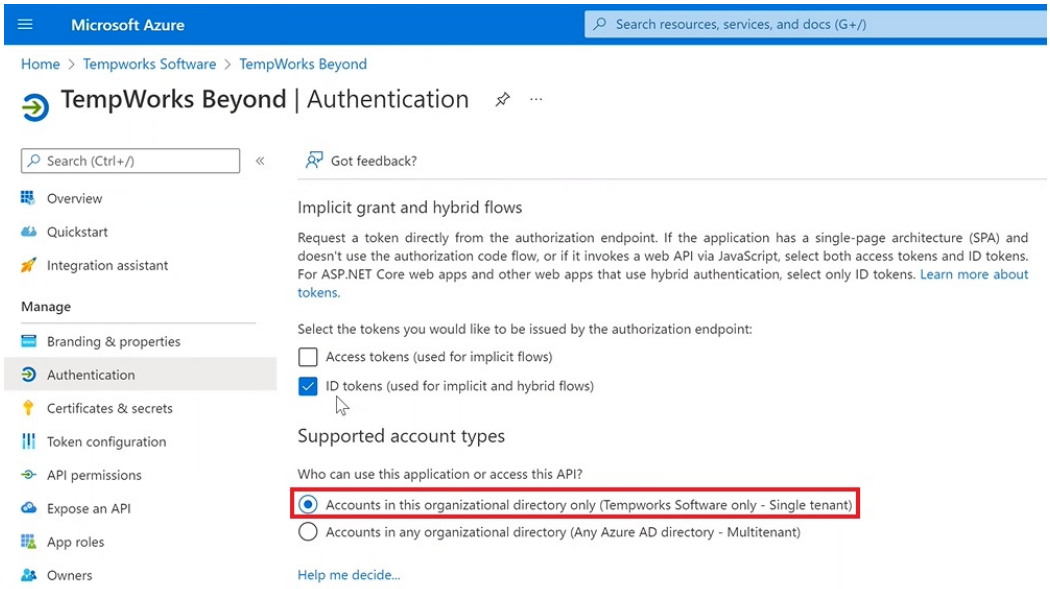


Paste the "Redirect URL" into the "Add URI" section.

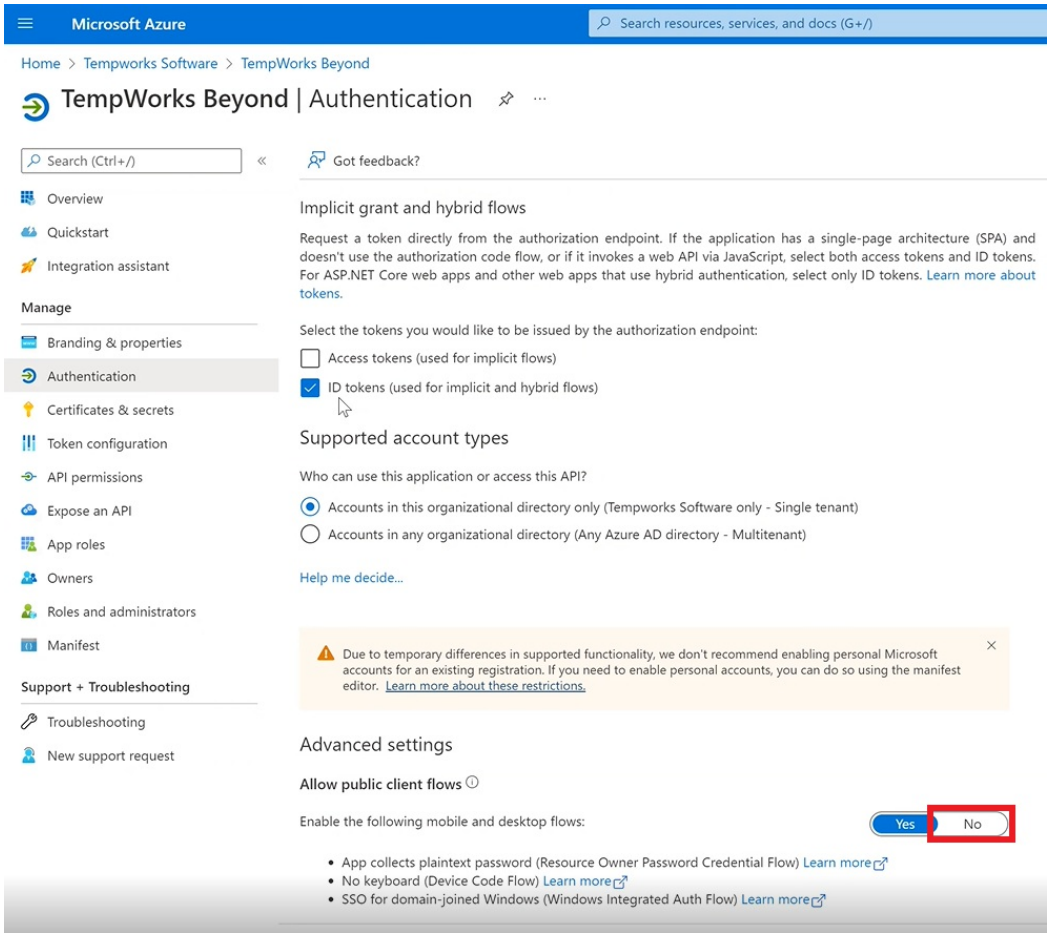
Check the box for "ID Tokens" within the "Implicit grant and hybrid flows" section:



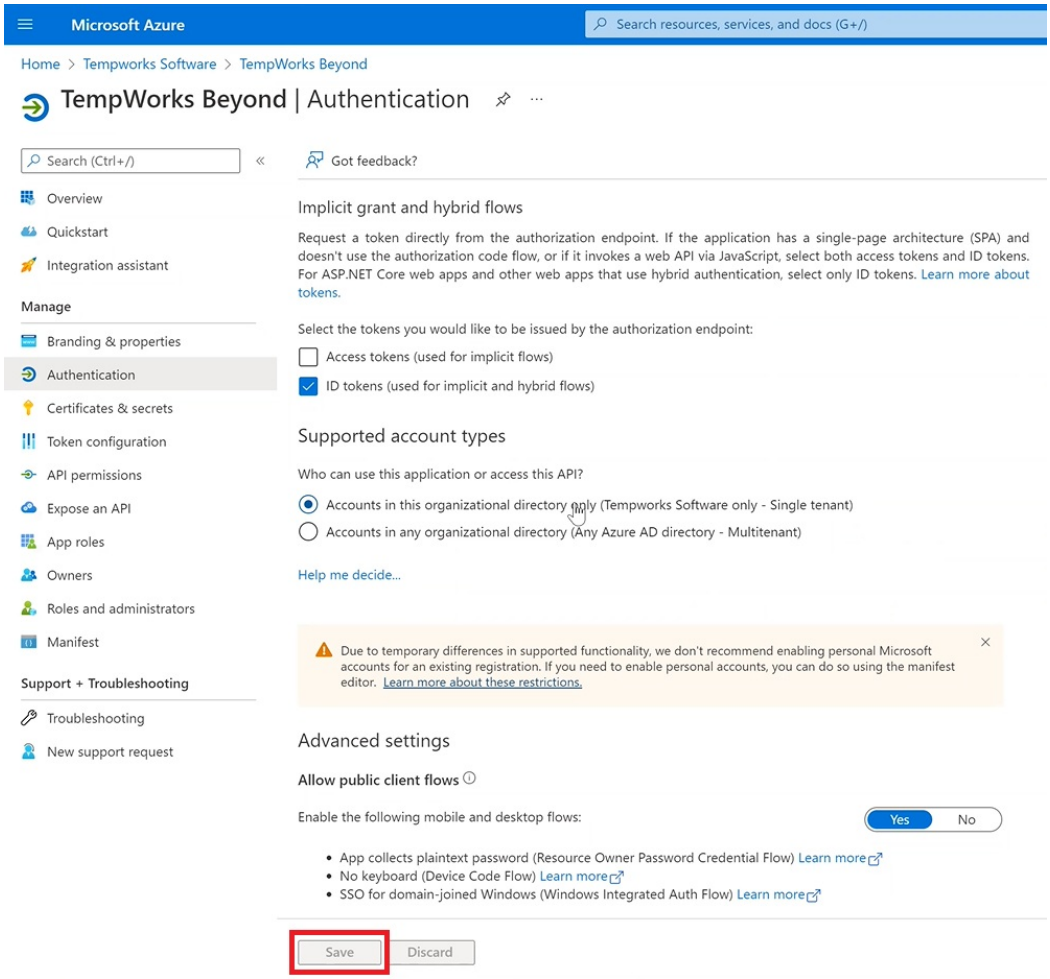
Select the option for "Accounts in this organizational directory only" within the "Supported account types" section:



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:



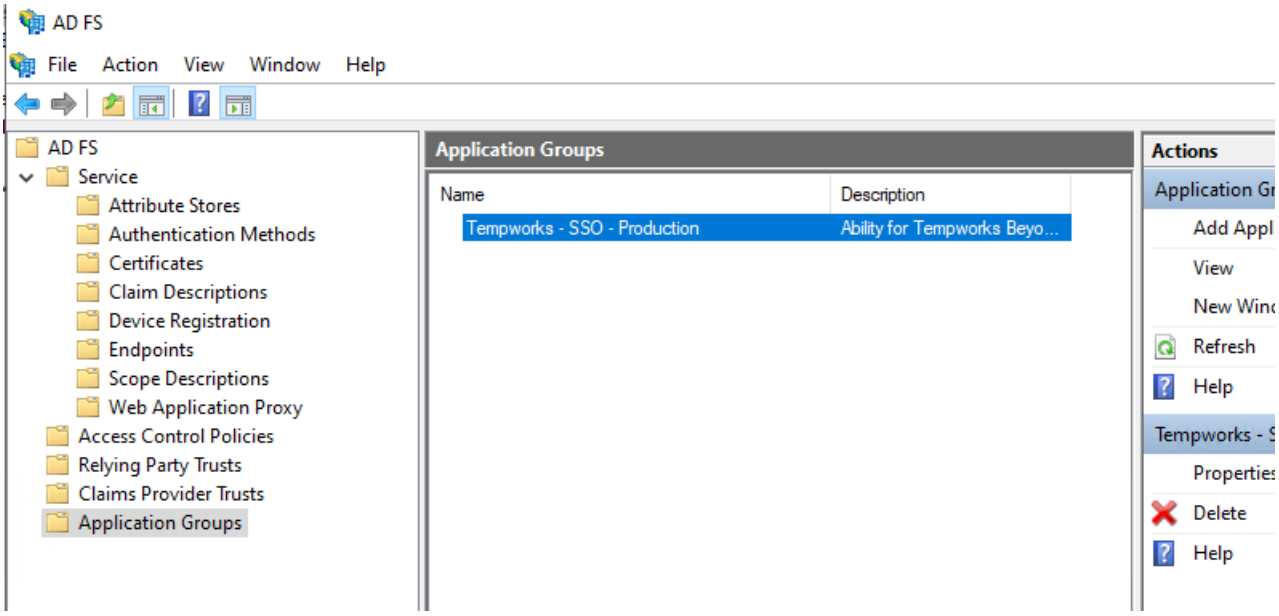
Once the Identity Provider setup is complete, you are ready to add the following information into Beyond and complete the setup of SSO:

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

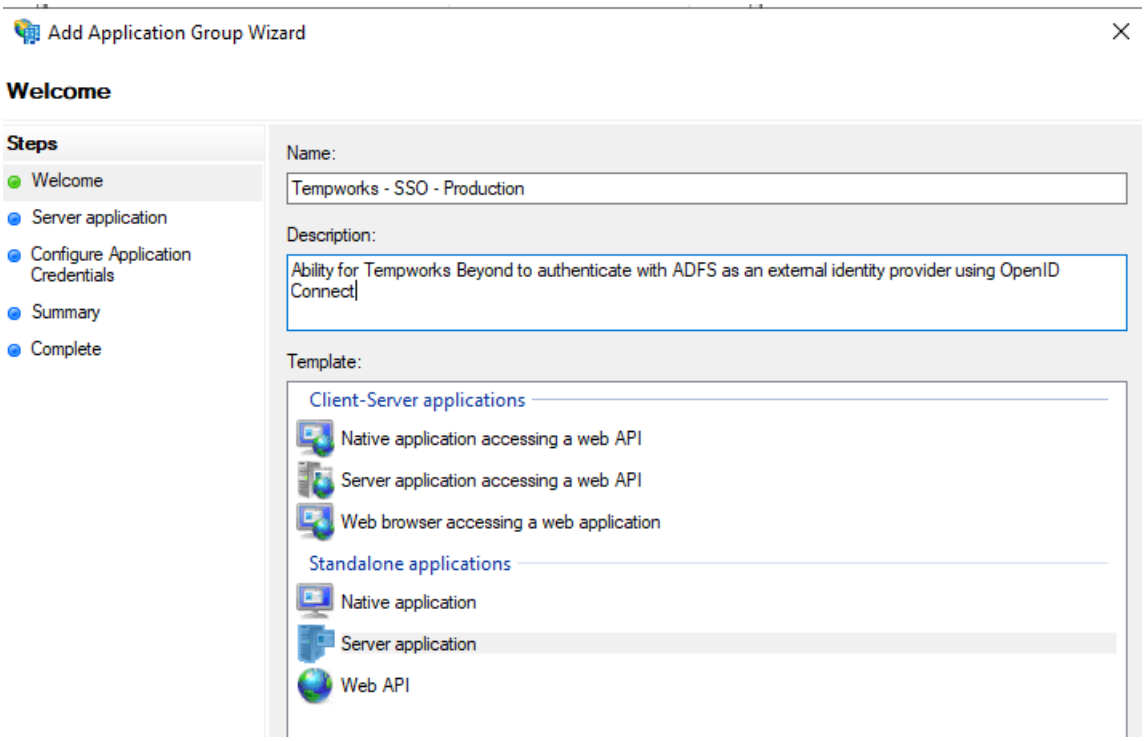
Note The following setup process assumes you have the Federation Services role installed and configured to use OpenID Connect.

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



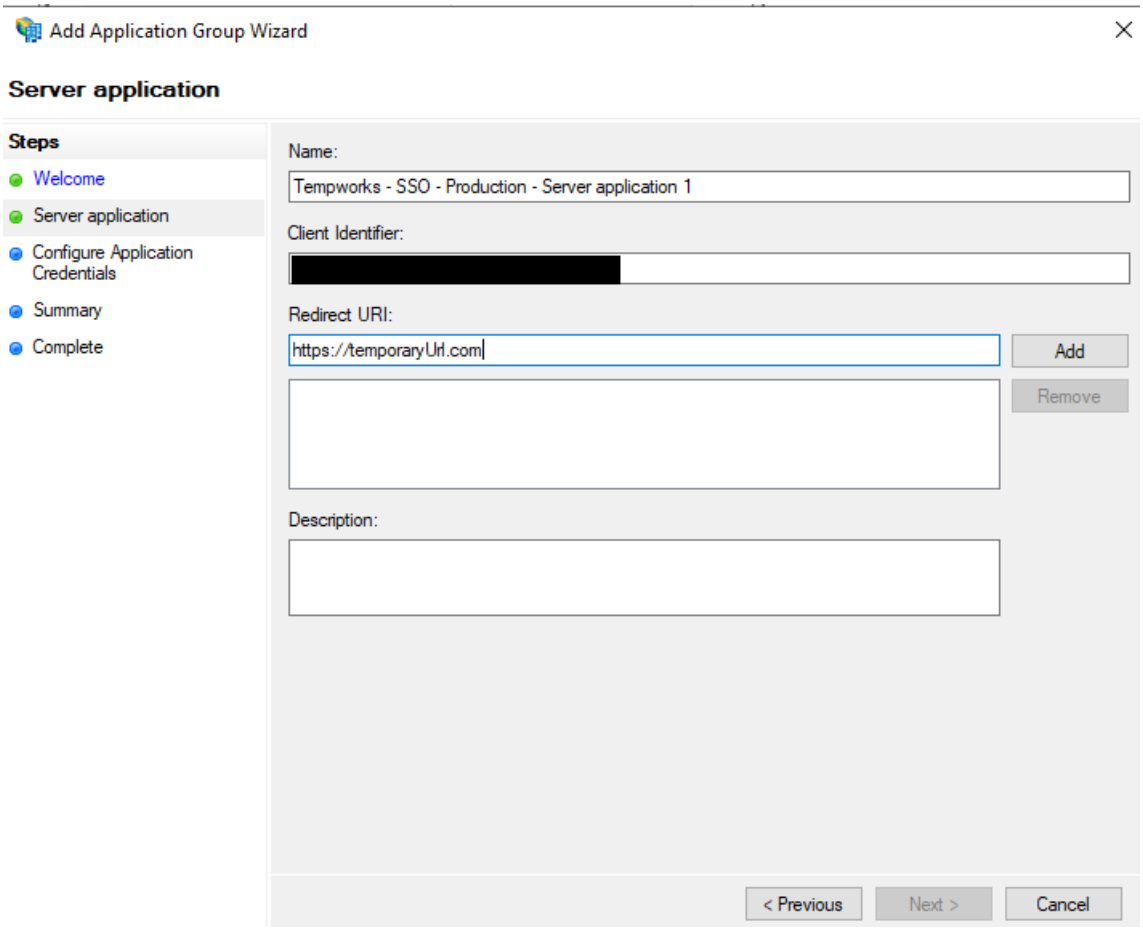
Select "Add Application Group" on the right and within the "Add Application Group Wizard", enter/select the following:

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



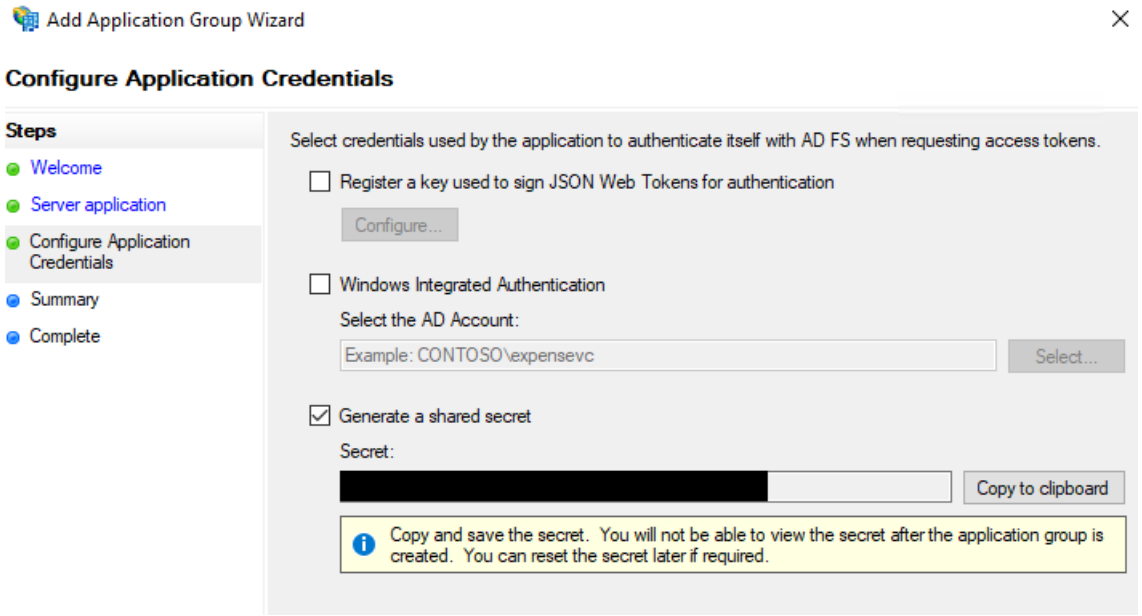
Select "Next" to add the application. Update the "Name" and/or "Client Id" as needed, but the generated GUID identifier can be used without issue:

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.



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

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



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

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.

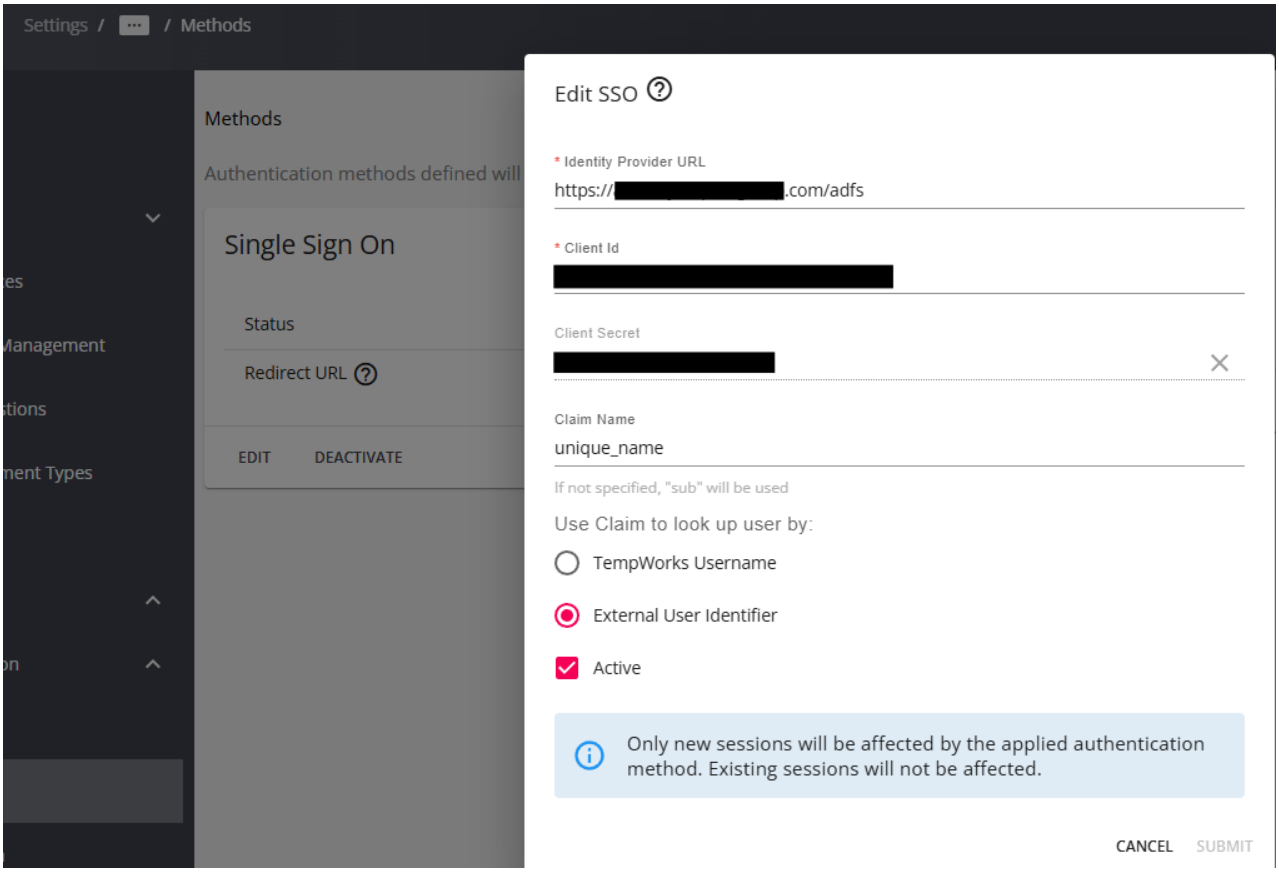
- **Client ID**: The "Client Identifier" from the ADFS setup process.
- **Client Secret**: The "Shared Secret" from the ADFS setup process.
- **Claim Name**: Enter "unique_name".
- **Use Claim to Look Up User By**: Select "External User Identifier".

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”.

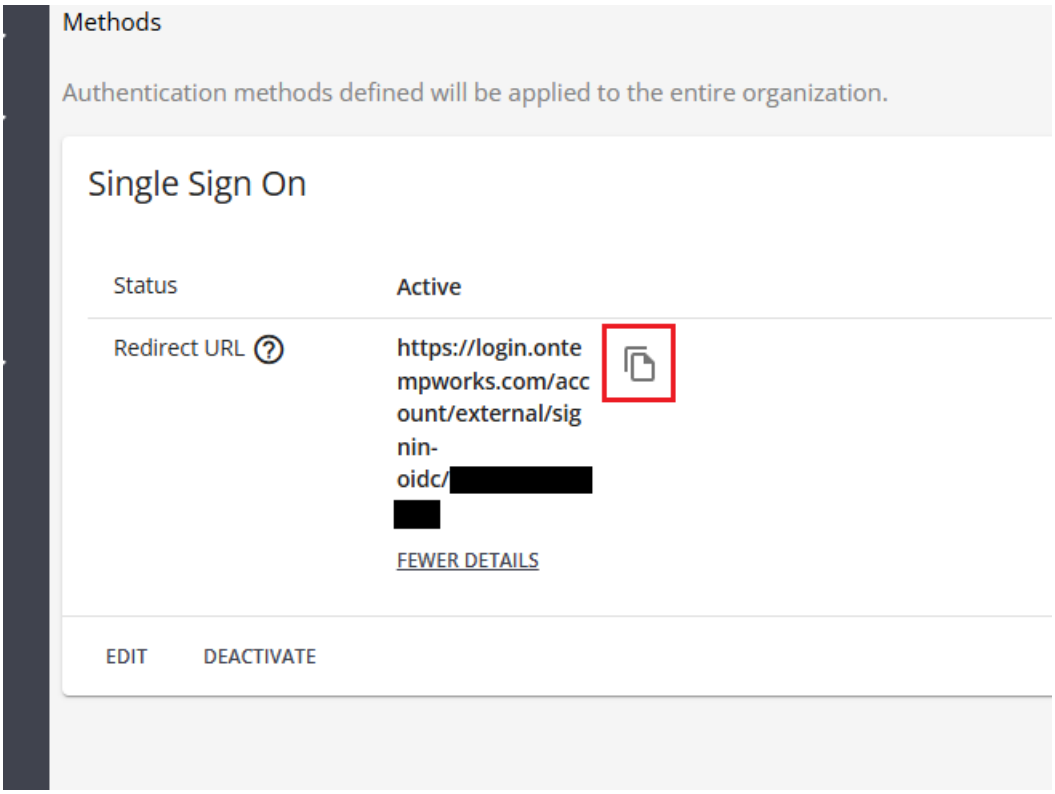
In the service rep settings for each user, the user’s domain username will need to be added to the “External User Identifier” field within B Menu > System Settings > Service Representatives.

- **Active**: Checked



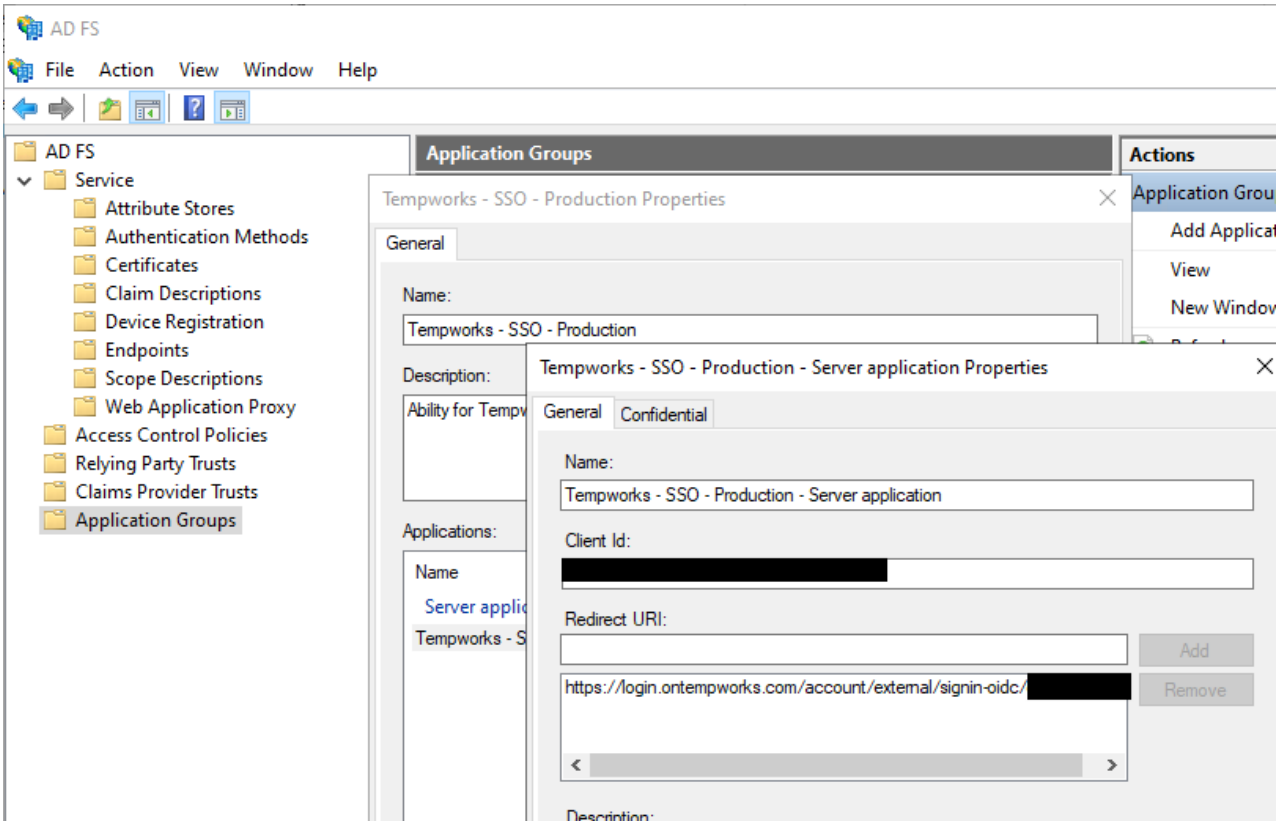
Select "Submit" to finalize the changes.

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



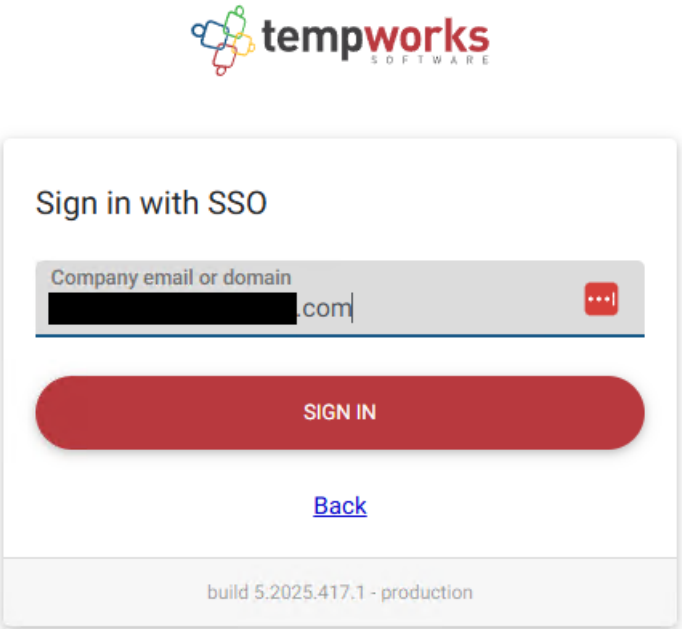
Navigate back to the ADFS Management UI and within the "Application Groups", navigate to the "Properties" of the Application Group you had previously created. Select "Edit" and replace the placeholder "Redirect URL" with

the URL generated from Beyond:



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:



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