Version 25

Trapeze
Enterprise Asset Management

# Single Sign-On (SSO)

Configuration Guide

**Trade Secret | August 2025**

**Technical Support**

Trapeze provides several ways to connect with the Customer Care team. Please provide detailed information to the representative. If you are reporting an issue by e-mail, include any error messages, screen shots of your problem, and steps to replicate the issue.

Customer Care is available Monday through Friday, 8:00 a.m. to 8:00 p.m., Eastern Standard Time.

| | |
|---|---|
| Toll-Free Telephone: | 1-877-411-8727 |
| E-mail: | cc@trapezegroup.com |
| FTP Site: | https://ftps.trapezegroup.com/ |
| Web Site: | https://collaborate.trapezegroup.com |

The website provides access to Trapeze Collaborate which offers resources to implement and operate the software, search knowledge, participate in communities, log/track service requests, sign-up for release alerts, view product health recommendations, and download updates or documentation. For secure access to Collaborate, contact Customer Care through the website or by calling the number above.

**Product Compatibility**

Refer to the latest Product Compatibility information on Trapeze Collaborate for requirements including operating system information, databases, Crystal reports, network protocol, HTTP servers and browsers that are supported.

# Single Sign-On (SSO) Configuration Guide

August 2025

## Contents

# 1. Overview

There are three areas you must configure to allow Single Sign-On:

1. Windows security settings/permissions to allow the correct authenticated users access to the website – this varies depending on the organization's security needs and settings. You may choose to use windows domain authentication, for example to allow only users in the domain to access the web server. With Single Sign-On, users typically are required to provide valid windows credentials (user, domain, and password) when first connecting to the web server, then are automatically logged into Web Modules based on whether their windows login is mapped to a user.

2. User setup via the GUI to set the **External identifier** field to map to a valid windows user ID, but only for the trusted users that have windows accounts on the server/domain.

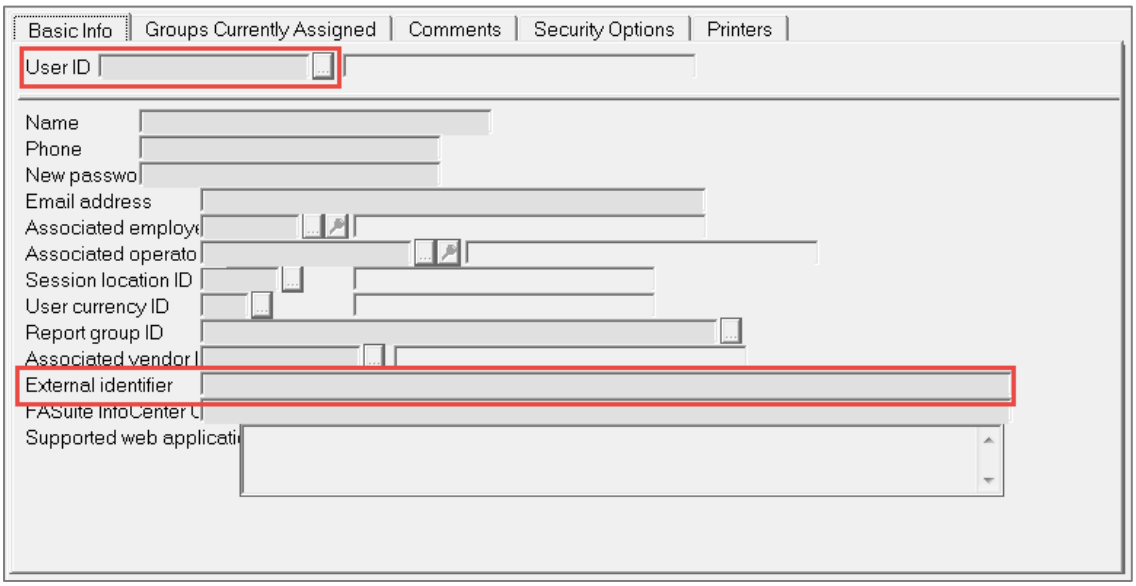
3. Web Modules settings via Configurator or manual IIS configuration if advanced settings are required.

⚠ MobileFocus, FuelFocus, and MAXQueue use different authentication methods and are not designed to work in an SSO environment. When configuring MobileFocus and FuelFocus, you must use a non-SSO web service URL. Please see the *MAXQueue Administrator Guide* for details on configuring MAXQueue.

# 2. Configure Single Sign-On (SSO)

## GUI User Setup for SSO Activation

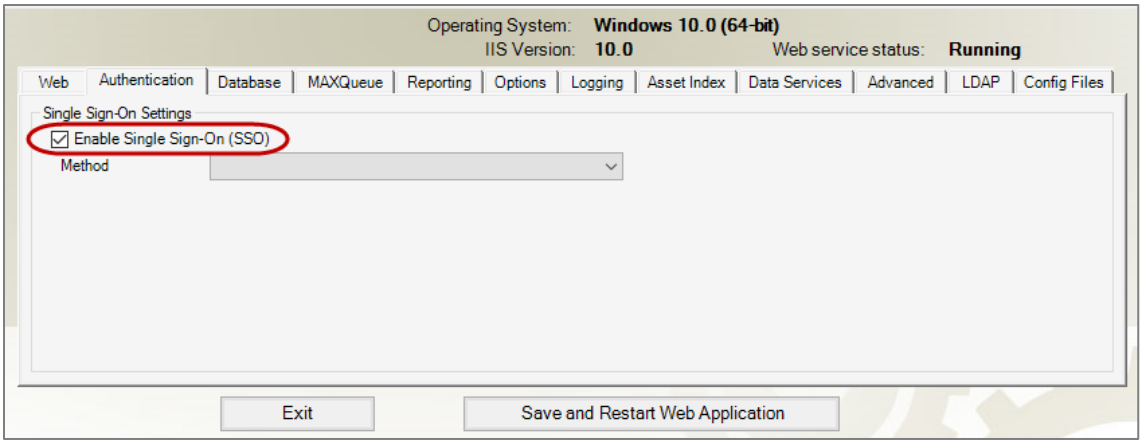
1. Start a GUI Instance.
2. Select **System Mgmt > Setup > Access Rights > Users**.
3. On the Basic Info Tab, enter the **User ID** for which you would like to enable SSO.
4. Enter the user's associated login name in the **External Identifier** field.




5. Save changes and exit the GUI.
6. Complete SSO activation through the Configurator as described below.

## Enable SSO via Configurator

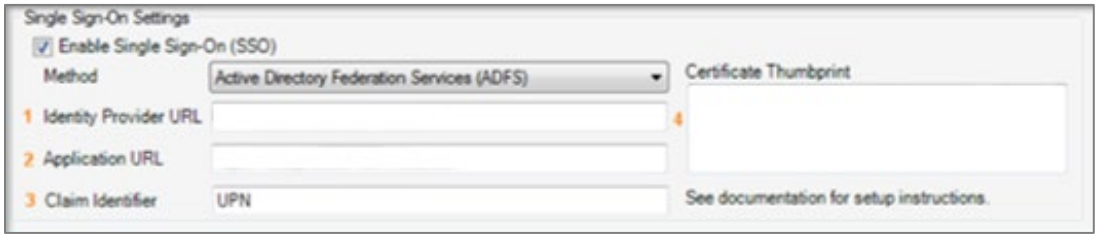
1. From the Authentication Tab, check **Enable Single Sign-On (SSO).**




2. Select the SSO **Method** from the drop-down list.

3. Follow instructions below based on method selected.

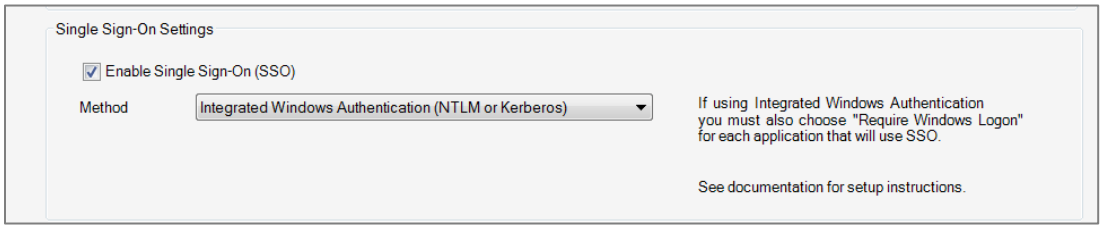
## ADFS – Active Directory Federation Services



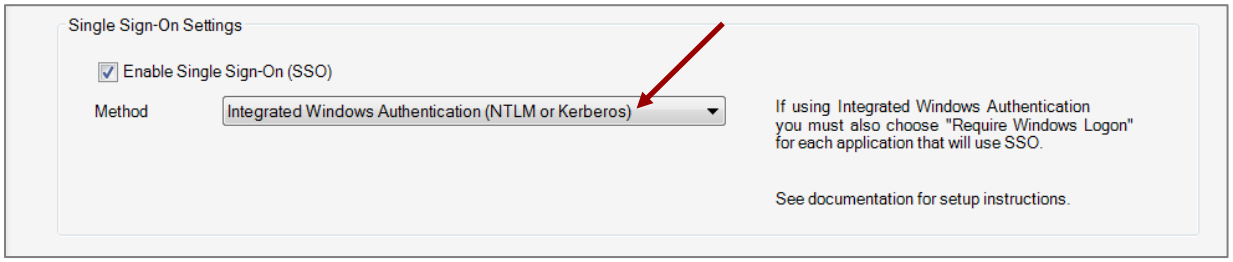

The following options are supported:

- Identity Provider URL (Required): The URL used to authenticate against the ADFS server
- Application URL (Required): The URL for the current Web Modules Instance
- Claim Identifier (Optional): The claim type the application will get from the ADFS server to map to an FA User (Default is UPN)
- Certificate Thumbprint (Required): The thumbprint of the signed certificate the ADFS signed. When entering a thumbprint, you must type in the code. Spaces and other text copied from another source will cause the authentication to fail.

## Kerberos or NTLM - Integrated Windows Authentication




Following is a high-level explanation of features and functions of the Kerberos or NTLM SSO.




### Launch URL

⚠ Be sure to use the correct Launch URL. Do NOT bookmark and use the frameset URL ("FASuiteInfoCenter.htm") or you may experience problems.

You should use only the Web Modules Application Launch URL, either the app path or the fully-qualified default:

- http[s]://<host>/<app>/
- http[s]://<host>/<app>/default.aspx

⚠ Do not use **http://<host>/<app>/FASuiteInfocenter.htm.** IIS Web App authentication settings.

### *Anonymous Access*

- DISABLED for Windows

### *Kerberos or NTLM - Integrated Windows Authentication*

- ENABLED for Windows

### *Forms authentication*

- ALWAYS ENABLED for Web Modules, regardless of whether SSO is used.

### *Product Features*

Initial Web Request when not yet authenticated in the product via SSO

- The Windows method supports automatically redirecting to the requested URL even when a user is not initially authenticated (as long as Windows SSO login is successful).

### *Single Sign-Off*

- Windows method does not support Single Sign-Off.
- It is possible to log off from Web Modules without logging off from the SSO provider. This is to support user impersonation and to prevent user confusion in the case of unexpected system errors and restarts.

### *User Impersonation*

- Windows supports product user impersonation (logging in as a user that is not associated with the current SSO user).
- To impersonate another user:
    - Logoff from Web Modules
    - Login using different credentials

***Automatic log-back-in***

This occurs when a user logs off from the product or the web session expires or is lost due to system error or web app restart.

- Web Modules does not support automatic log back in, but does support easy login via a hyperlink on the login form **Login as X** (where X is the username mapped to the currently authenticated SSO user)
- Recommended method for logging back in automatically is to close all open web browsers and reopen browser to the product's URL.
- The *SSO* re-login feature is enabled by default, but it can be disabled by editing fasuite.config to set key *FASuite.Web.SingleSignOn.AllowRelogin = False* (this option is not available in Configurator).

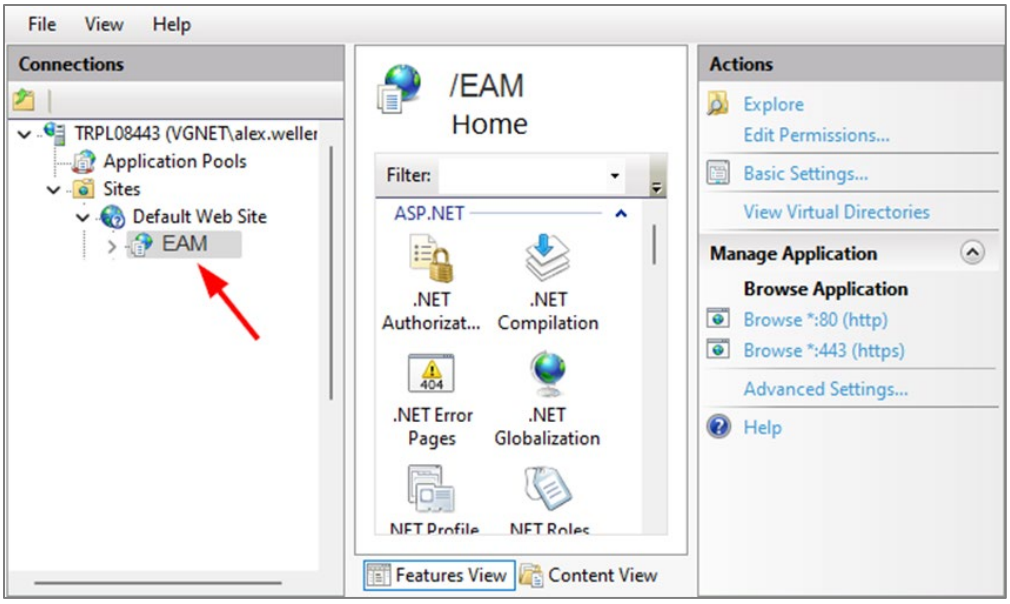
## Enable Kerberos or NTLM - Integrated Windows Authentication via IIS

Most of the steps performed automatically by selecting the SSO method in the Configurator program can also be manually performed in IIS. You will still need to select Kerberos or NTLM - Integrated Windows Authentication in the Configurator and click the "Save" button.

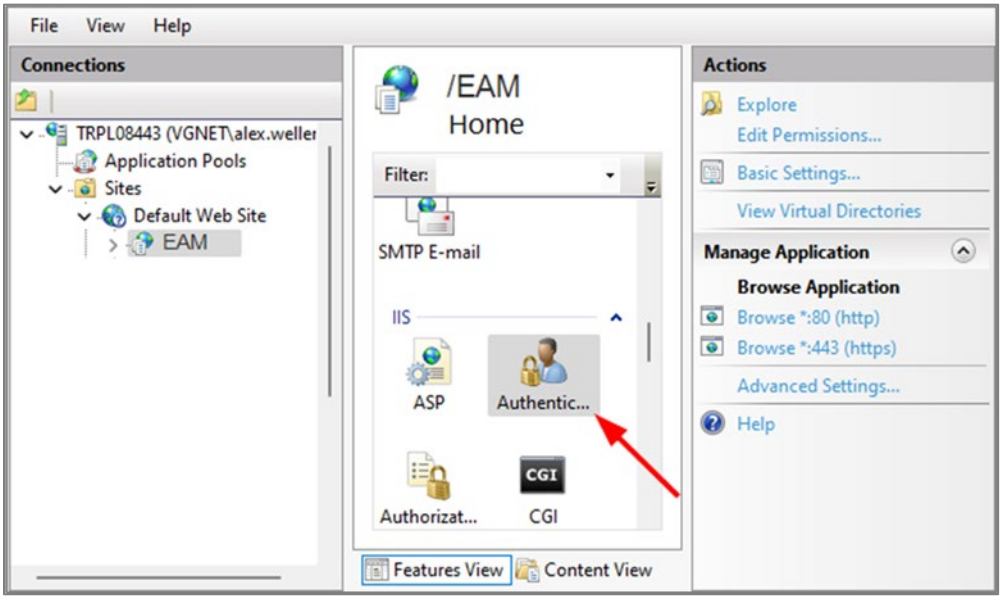
The following steps will cover what manual configurations can be applied in Internet Information Services (IIS) to enable Windows Authentication SSO.

**To allow automatic sign-on to Web Modules:**

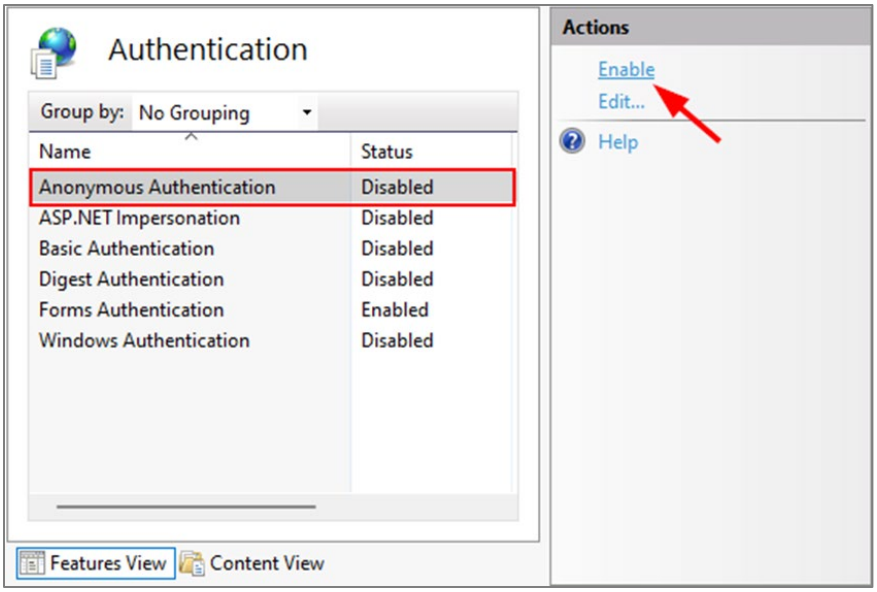
1. Disable Anonymous Access for the Internet Information Services (IIS 7.0) of your Web website application.
2. Open your IIS manager.
3. In the Connections pane, select the web application that you configured earlier for the Web site (EAM).



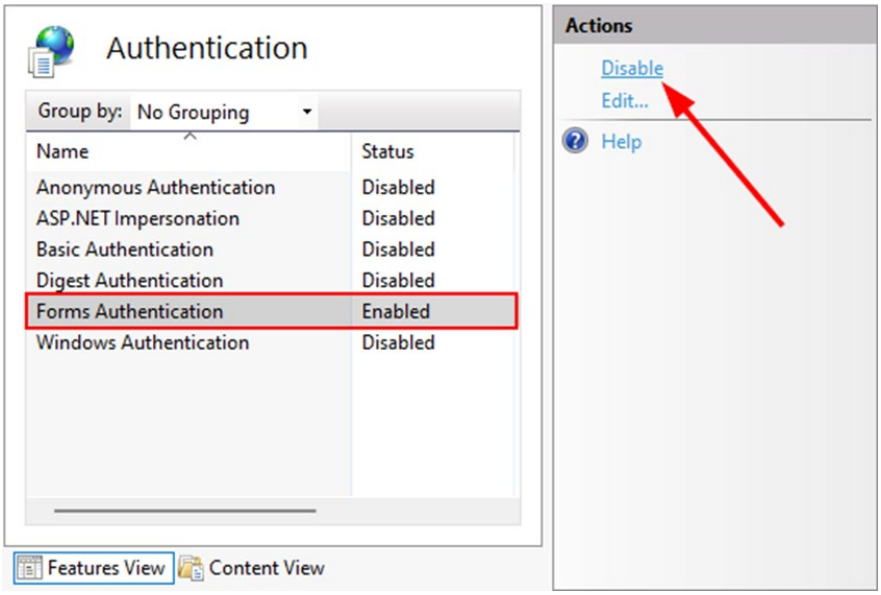

4. Double-click **Authentication** in the features view, as shown below.



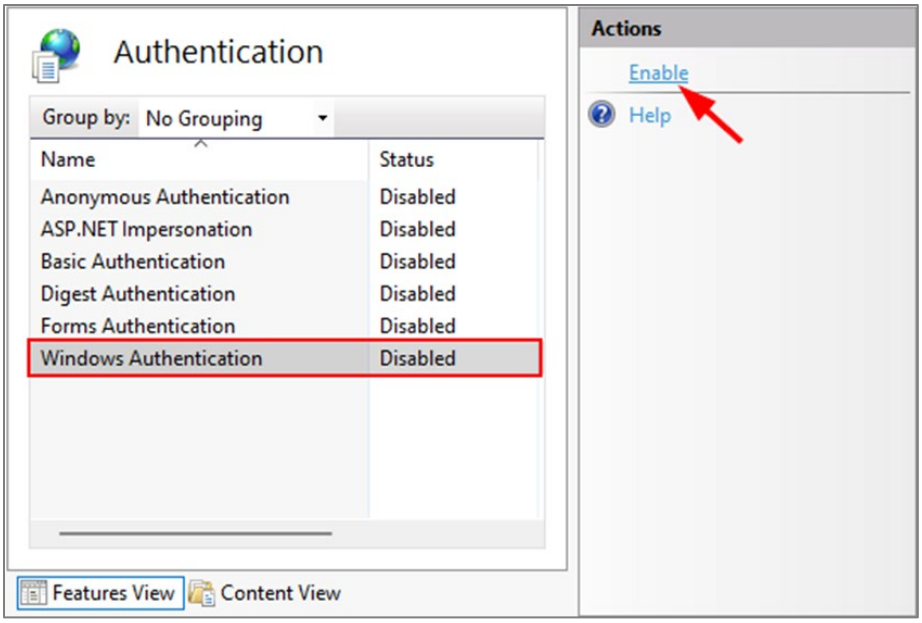

5. Make sure that **Anonymous Authentication** is **Disabled.** It should be enabled by default.



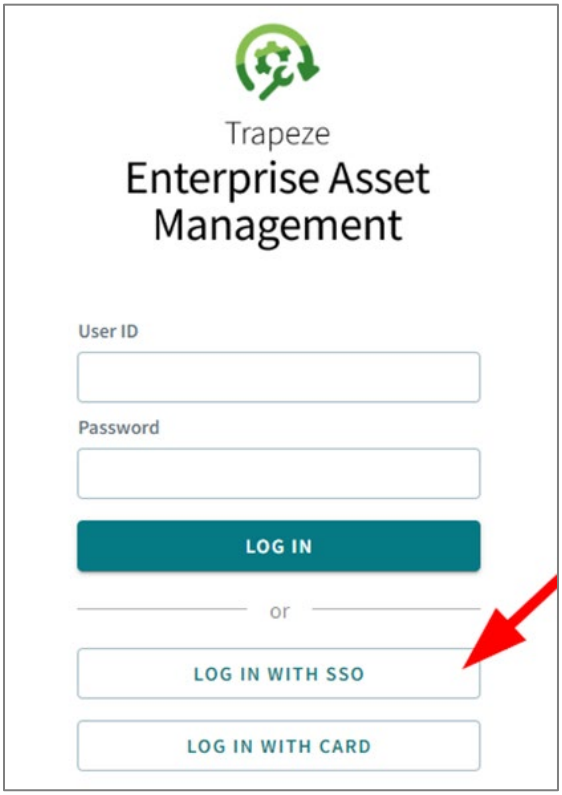

6. Make sure that **Forms Authentication** is **Disabled**. It should be enabled by default.




7. Make sure that **Windows Authentication** is **Enabled**. It should be disabled by default.




An additional feature that is included when Single Sign-On in enabled is a button provided to sign the user in using the currently configured Single Sign-On method.



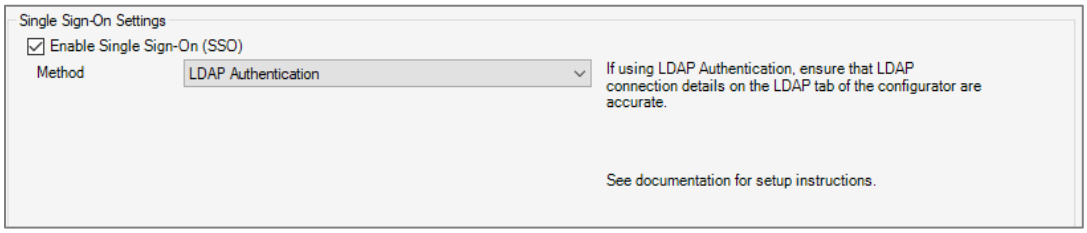
# LDAP – Lightweight Directory Access Protocol

## Import LDAP Users

When configured, system administrators will be able to tell the system to import user data from their network's LDAP server (typically will be an Active Directory server, but any directory service implementing the LDAP protocol will work). They will be presented with a table of users that have been pulled from the connected server and who's data is different from the data in the system. This user data can differ in one or more of the following ways:

- User does not exist in the system
- Username is different
- Phone Number is different
- Email Address is different
- User Group membership is different

The administrator is then able to review the available users for import, select the ones they want and click **Import Selected Users** to update the user records in the system with that information. In this table, the fields that differ from system fields will be highlighted red. There is a legend below the table indicating what this color means.




When this option for SSO is turned on in the configurator, users will be able to enter their domain user and password and have the authentication and authorization happen in the connected directory instead of internal to the system. This method is also supported for MobileFocus using Data Services.

The workflow for this authentication works as follows:

1. The user enters their domain user and password in the system login form or MobileFocus login form and clicks **Login**.
2. The system or Data Services attempts to connect to the configured LDAP server with these credentials.
3. If successful, the user is authenticated but further verification is required to determine that they are allowed access to the system.

4. The system or Data Services re-connects to the directory service as a user that has rights to query user data from the directory service. It runs a search using a filter provided in the configurator. If the current user's UserID exists in the filtered set of users, then they are granted access to EAM.

Refer to the LDAP Tab section for additional information.

## OAuth 2.0 - Open Authorization 2.0

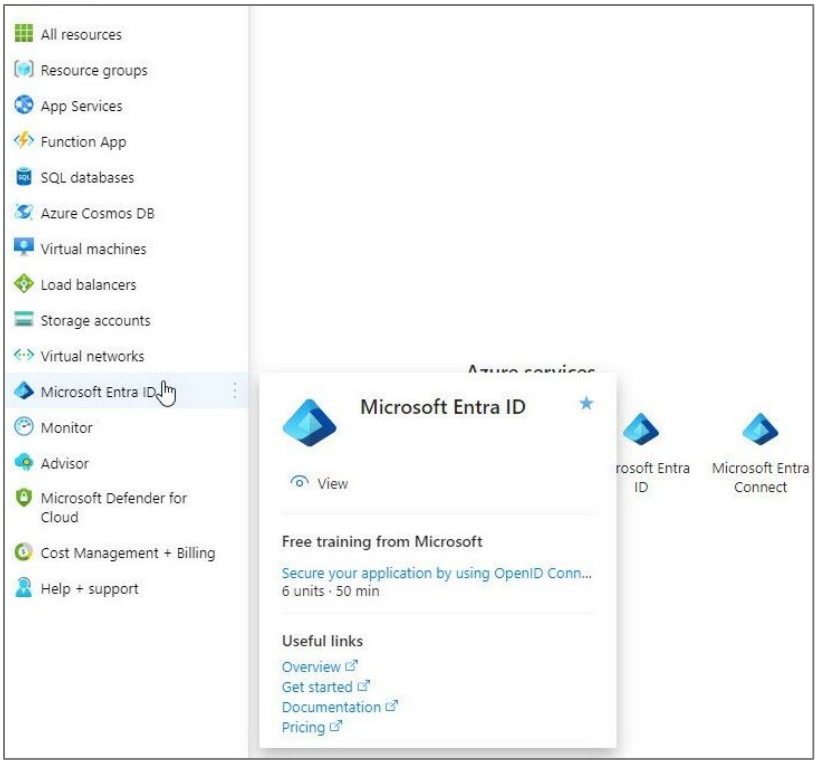
### Prerequisites

- OAuth 2.0 - Open Authorization 2.0
- account and administrative access to portal
- Configured users in OAuth 2.0 - Open Authorization 2.0
- UPN claim (User principal name) to be used to uniquely identify users in Microsoft Entra
- EAM configured to work with HTTPS where a valid/trusted certificate is being used

## OAuth 2.0 - Open Authorization 2.0 Configuration

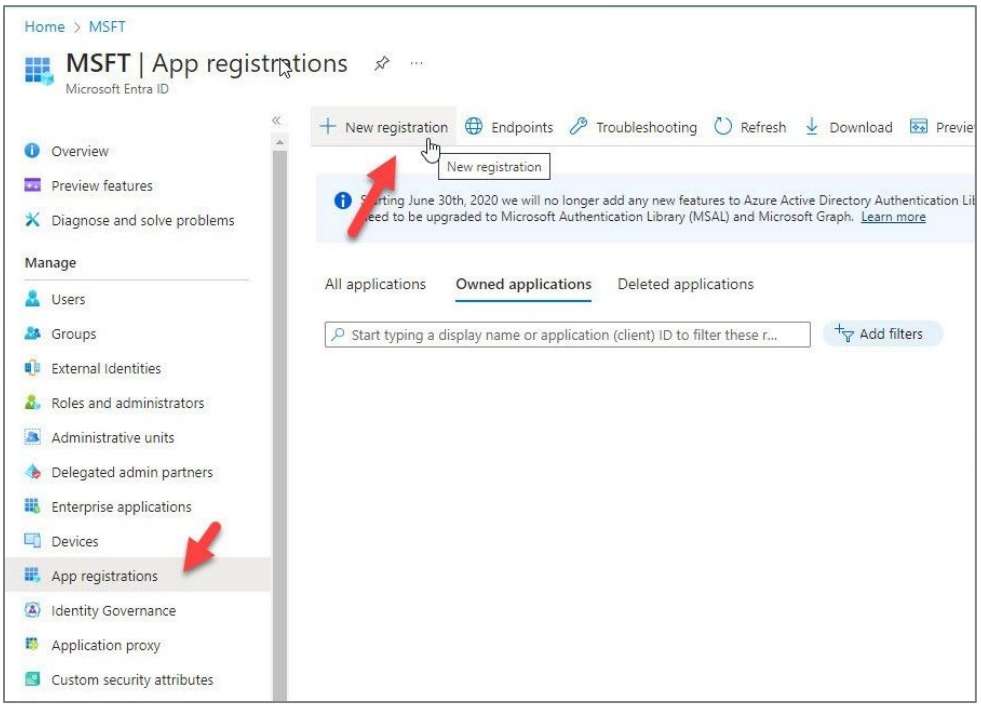
The EAM application will need to be registered with the OAuth 2.0 - Open Authorization 2.0 service so that it is allowed to authenticate its users.

1. Access the OAuth 2.0 - Open Authorization 2.0 tenant.
2. In the panel of services on the left, select **OAuth 2.0 - Open Authorization 2.0**.

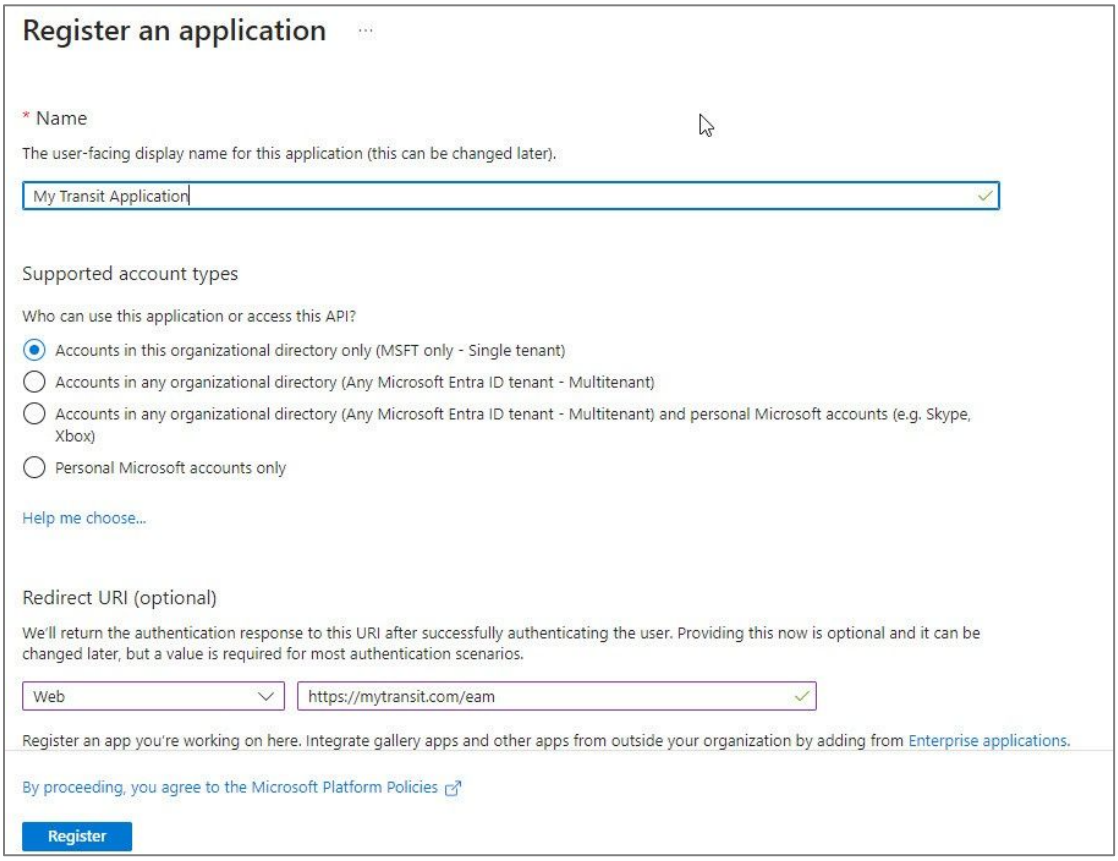



## Register The Application

1. In the second nested panel of OAuth 2.0 - Open Authorization 2.0 actions, select **App registrations**.



2. To create a new web application, click the **New registration** button at the top of the main display. This will allow you to register a new application in your OAuth 2.0 - Open Authorization 2.0.

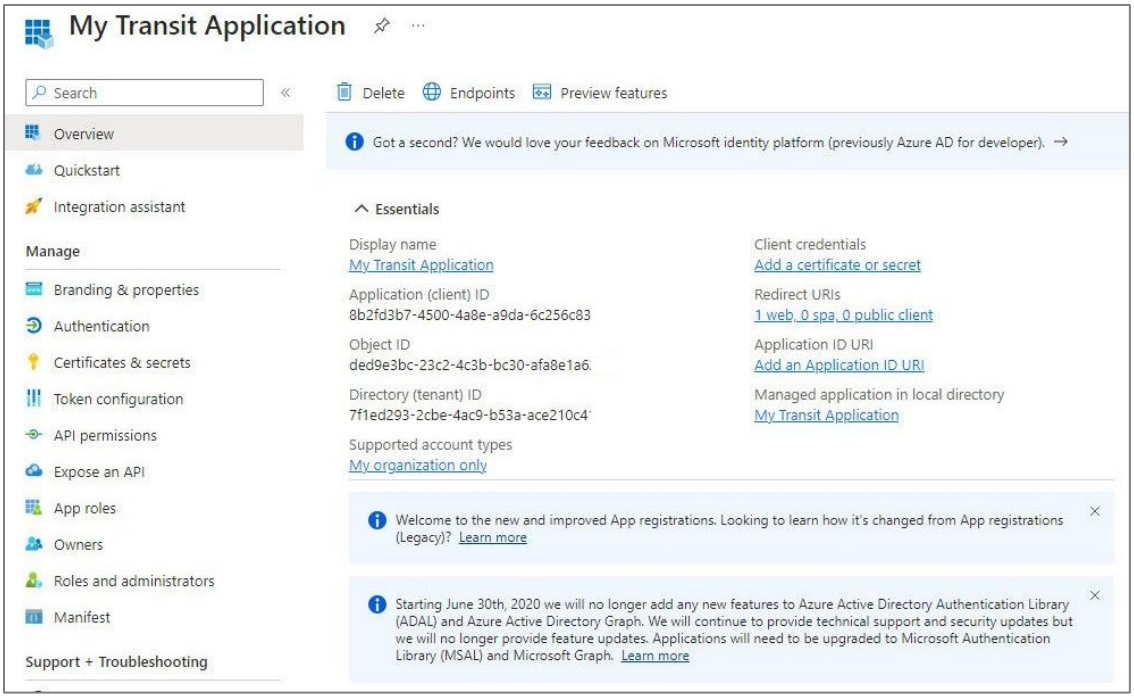



3. Enter a name for your EAM application (for example, EAMPROD, EAMTEST, EAMDEV).

4. Configure who may use the application. For most customers, your single tenant directory will suffice.

5. Optionally, enter your first Redirect URI at this point. This is a URL where OAuth 2.0 - Open Authorization 2.0 will allow your browser to be redirected. It is the URL used to access your EAM Web Modules or Data Services applications. It will also need to match the callback URL you enter in your Configurator so note your entry for later use. Alternatively, this may be done later in the process.

6. Click the **Register** button to register the application.



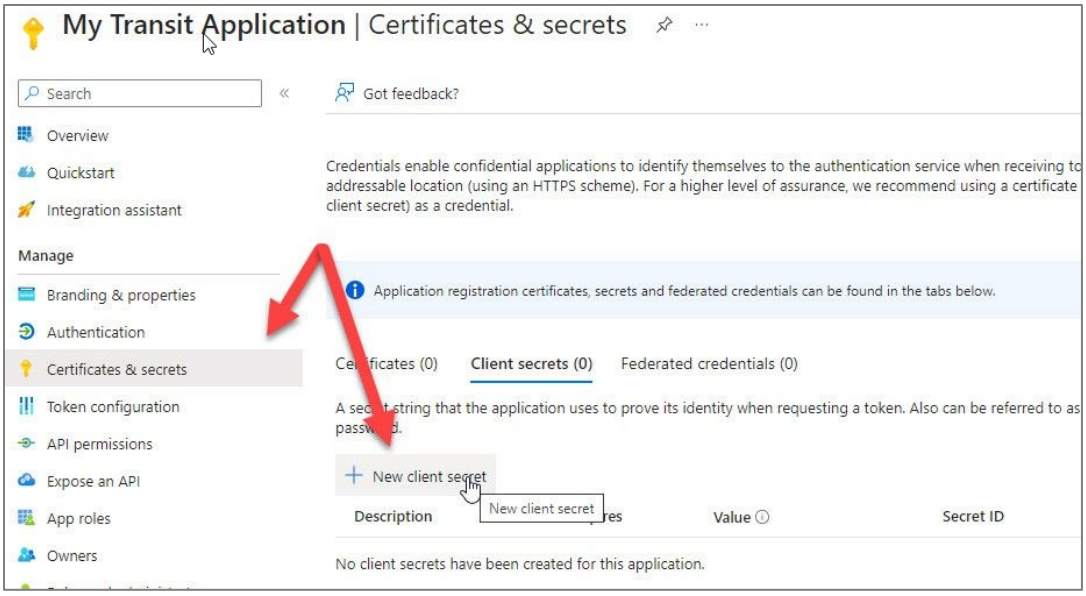

The application has now been registered successfully.

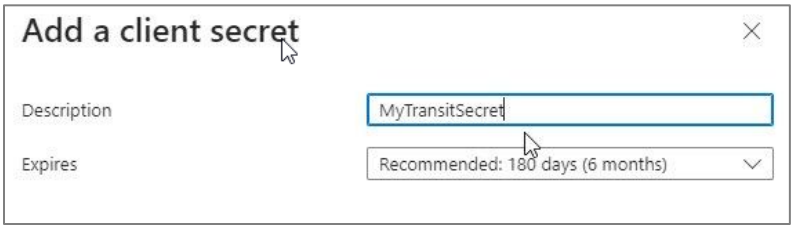
Make note of the **Application (client) ID** and **Directory (tenant) ID** values as they will be needed later in the process.

## Create Application Secret

Next, create the Application Secret. This is a key that will allow OAuth 2.0 - Open Authorization 2.0 to trust the EAM application.

1. Click on **Certificates & Secrets**.
2. Under the **Client Secrets** section on the main display, click **+ New client secret**.



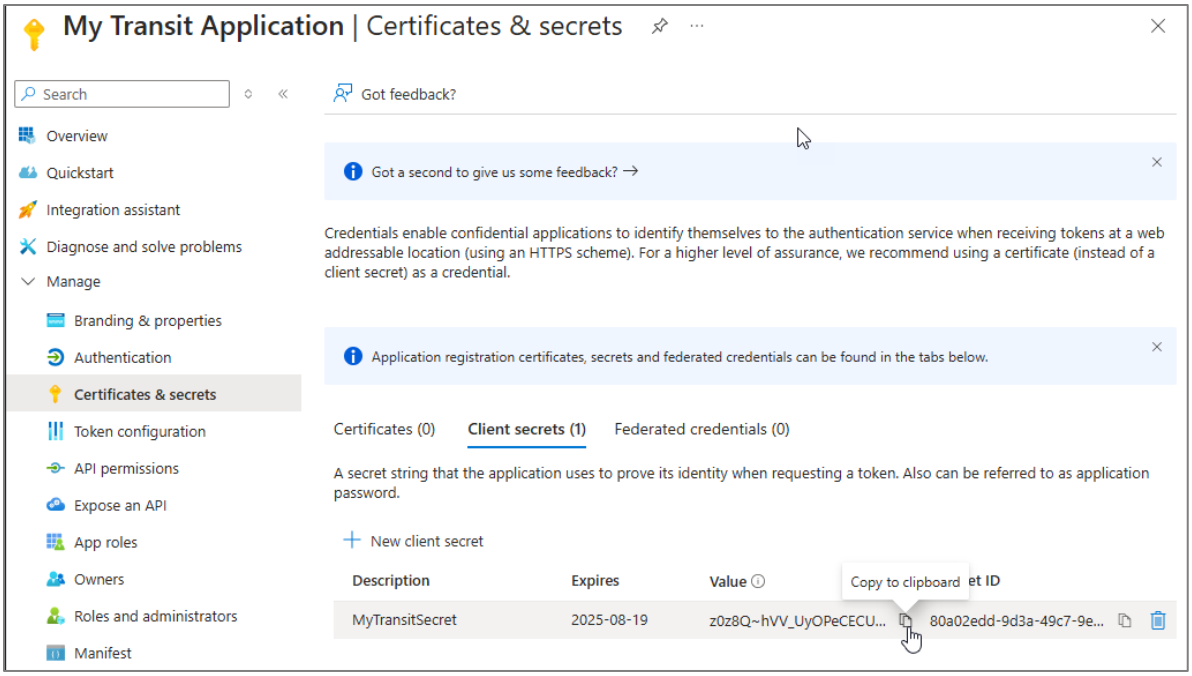




3. Enter a description for this secret.
4. Enter the expiration window you would like.
    i. The shorter the window, the more secure it will be.The higher the window, the less secure it will be allowing more time for someone to intercept the secret and impersonate EAM.

        This is a secret that you will need to maintain so contact your IT department or System Admin and notify them of the expiration window that is configured. They will need to generate new secrets AND reconfigure EAM to use them before the currently active secret expires. If the currently active secret does expire, OAuth 2.0 - Open Authorization 2.0 will not trust EAM and users will not be able to sign in.

5. Click **Add** and your secret will be created.
6. Copy the Secret Value (may use clipboard icon next to it for convenience) and store it for later use.

    Before moving on to doing any further steps, copy the secret. <u>This is your ONE chance to copy this, do not ignore this step.</u>

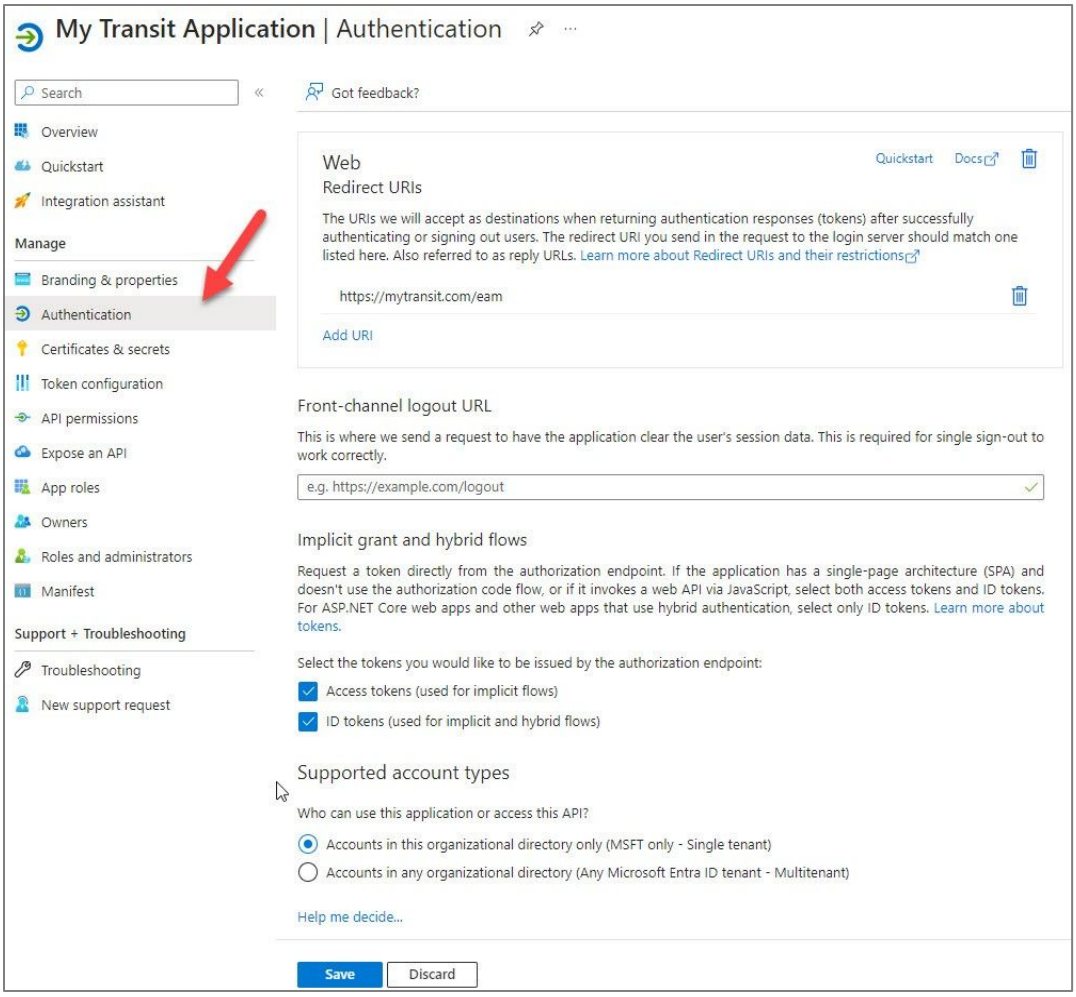



## Register Additional Redirect URLs

After successfully authenticating and authorizing a user, OAuth 2.0 - Open Authorization 2.0 will redirect the user's browser back to EAM. As a security feature, it will not redirect to just any URL that is passed to it, it must be pre-configured in a whitelist to be allowed.

In the **Register the Application** section mentioned above, you may have already provided one callback URL while registering the application. If you did not do that, or you wish to setup additional URLs (for example, running multiple Web Applications with distinct URLs), follow these steps to support them:

1. Click the **Authentication** tab.




1. For each URL that a user or device will need to access, configure it in the **Redirect URIs** section by clicking **Add URI** and entering the URL.

   Note: Ensure there are no trailing slashes on the URL.

2. Front-channel logout URL.

   i. EAM currently does not support logout URLs.

3. In the **Implicit grant and hybrid flows** section, check the checkboxes for both **Access Tokens** and **ID Tokens**.

4. For **Supported account types**, use the default single tenant option.

5. Click **Save** at the bottom of the page.

## EAM Configuration

### *Configure Users in EAM*

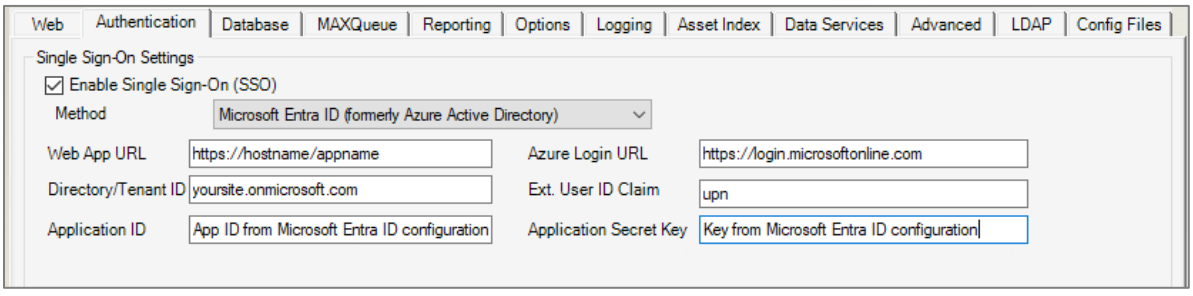
Before altering any settings in the Configurator, configure EAM User accounts to be capable of consuming the OAuth 2.0 - Open Authorization 2.0 integration.

1. Log into Web Modules.
2. Open the Users screen.
3. For each user that you want to use OAuth 2.0 - Open Authorization 2.0, edit their **External identifier** record, and enter their domain account (for example, MyUser@MyTransit.com).
4. Check the **Requires external authentication** checkbox on the **Security Options** tab. Enabling this will prevent direct sign-in to EAM. It will force the user to sign in through OAuth 2.0 - Open Authorization 2.0 SSO.
5. Save and repeat for any users you wish to setup.

### *Update Configuration with OAuth 2.0 - Open Authorization 2.0 Settings*

Next, configure EAM for OAuth 2.0 - Open Authorization 2.0 Single Sign-on.

1. Remote into the VMs/Servers that run a Web Modules or Data Services application. If multiple Web Modules products are installed, each will need to be configured individually.
2. Launch the Configurator.exe program. Currently, the Web Modules configurator supports configuring Single Sign-on. If you have a Data Services install, it will need to have a Web Modules product installed in the same deployment so you can use the Web Modules configurator (it will configure Data Services as well as Web Modules).
3. Click on the **Authentication** tab.
4. Check **Enable Single Sign-on (SSO).**
5. Select **OAuth 2.0 - Open Authorization 2.0** in the dropdown list.



6. Configure the available fields:

    i. **Web App URL** - This is the URL where OAuth 2.0 - Open Authorization 2.0 will redirect the user's browser to. This will be the URL to this specific Web Modules IIS website and will have also been one of the "Redirect URLs" that you configured while configuring OAuth 2.0 - Open Authorization 2.0. Https is required for this. Using an http URL is not supported.

    ii. **Azure Login URL -** This should not need to change but is made available in case Microsoft changes their login endpoint. It is the URL that EAM will redirect the browser to for the User to login.

    iii. **Directory/Tenant ID -** This is the value that was copied earlier when we first registered EAM in OAuth 2.0 - Open Authorization 2.0. It will typically be in a GUID/UUID format.

    iv. **Ext. User ID Claim -** The default of "upn" will be acceptable for most customers. This is the property on the user record in Active Directory to pull the UserID from to sign into EAM.

    v. **Application ID -** This is the value that was copied earlier when we first registered EAM in OAuth 2.0 - Open Authorization 2.0. It will typically be in a GUID/UUID format.

    vi. **Application Secret Key -** This is the value that was copied earlier when a secret for the EAM application in OAuth 2.0 - Open Authorization 2.0 was created. Do not share this with anyone. As a reminder, this key will periodically expire, so when your IT/System Admin generates a new key in OAuth 2.0 - Open Authorization 2.0, they will need to enter the new secret key value in this textbox for each EAM application configured to use OAuth 2.0 - Open Authorization 2.0.

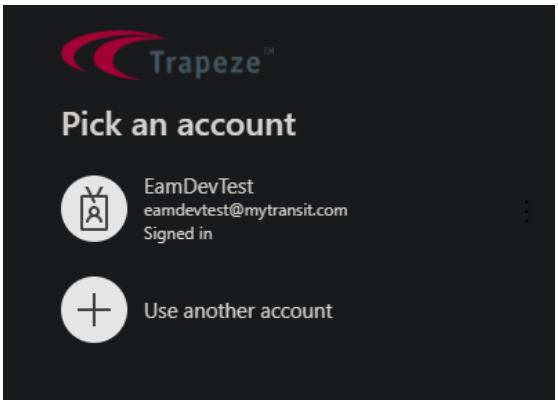
7. Click **Save**.

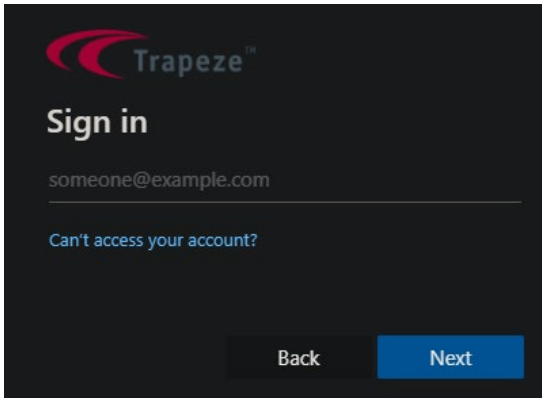
## Logging into EAM via OAuth 2.0 - Open Authorization 2.0

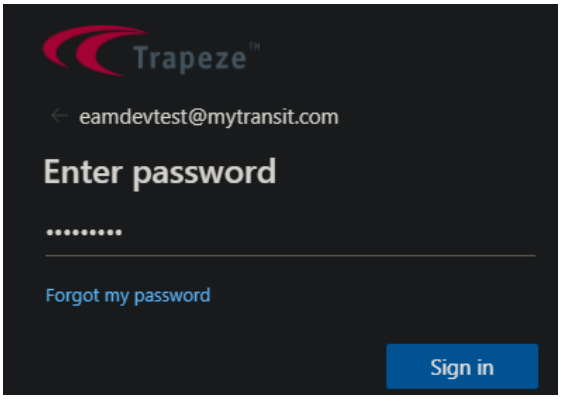
Now that both OAuth 2.0 - Open Authorization 2.0 and EAM are configured, the SSO integration should be able to be successfully exercised.

1. Launch your browser and navigate to Web Modules.

2. The first time will require you to login. Rather than seeing EAM Web Modules, the browser will be redirected to the OAuth 2.0 - Open Authorization 2.0 login page.



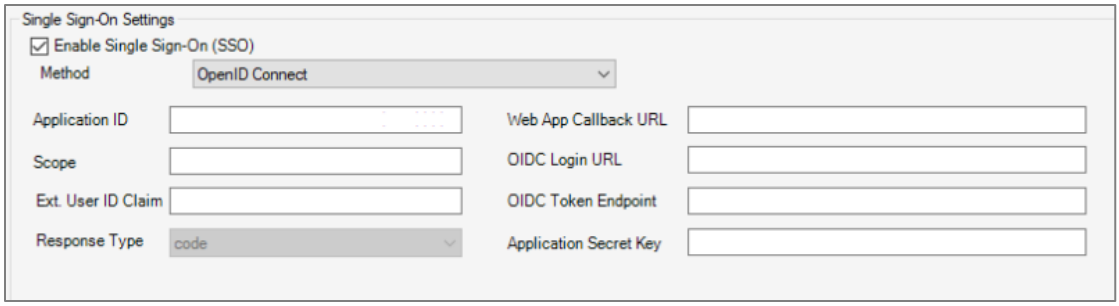




3. If it is the first time a user is accessing EAM via OAuth 2.0 - Open Authorization 2.0, they may be prompted with an additional view asking if they will allow the application to read their data. Grant access as this is required for EAM to read the UserID from OAuth 2.0 - Open Authorization 2.0 that will be signed into EAM.

4. Web Modules will then look up the related user record in Trapeze EAM and sign that user in.

## OIDC - OpenID Connect

When users open the Web Modules using OpenID connect for authentication, if they are not authenticated, they are redirected to the IDP (Identity Provider). From the IDP, the user is prompted to log in and authenticate. If this is successful, the user is redirected back to the Web Modules, which create a back-channel post sending over the code and the secret key assigned by the IDP. The IDP then sends an access and ID token back to the web modules which extracts the external user ID and attempts to look up the user (external ID is mapped to a valid application user) and log them in.




Fill out the following fields to set up OpenID. Some of the following fields are supplied by the identity provider (IDP).

- Application ID: The unique code to identify the application. This information is sourced from the IDP.
- Scope: OpenID must be one of the values entered here. Enter any other required and optional scope values. This information is sourced from the IDP.
- Ext User ID Claim: After the id_token is returned to the application; this is the claim used to parse the token to extract the external ID. This information is sourced from the IDP.
- Response Type: Code is the only option supported
- Web App Callback URL: Enter the application URL. This must be followed by the */Default.aspx*. For example: *https:localhost/infocenter/default.aspx*. This can be found on the Web tab.
- OIDC Login URL: The URL to prompt the user to authenticate against the IDP.
- OIDC Token Endpoint: The URL to post the code received from the IDP that returns the id_token. This information is sourced from the IDP.
- Application Security Key: The key used to post to the token endpoint. This information is sourced from the IDP.

# Single Sign-On Browser Configuration

This section provides instructions for single sign-on (SSO) browser configuration using Internet Explorer.

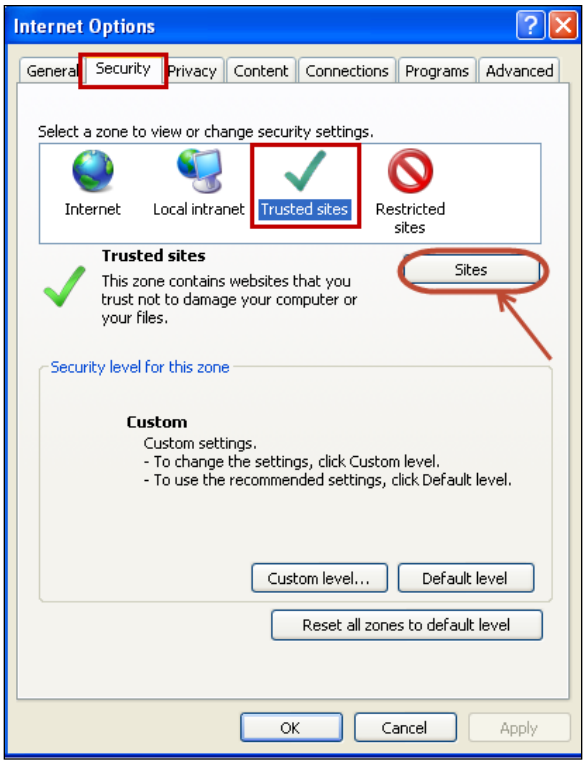
Adding the host (web server IP or hostname) to your trusted sites ensures the following features work better:

- Automatic single sign-on
- File uploads and file links using absolute pathname
- Enterprise Portal (and other pop-up windows) shows correct title bar

- Pop-up blocker issues fixed Single Sign-On

**To configure your browser for Single Sign-On:**

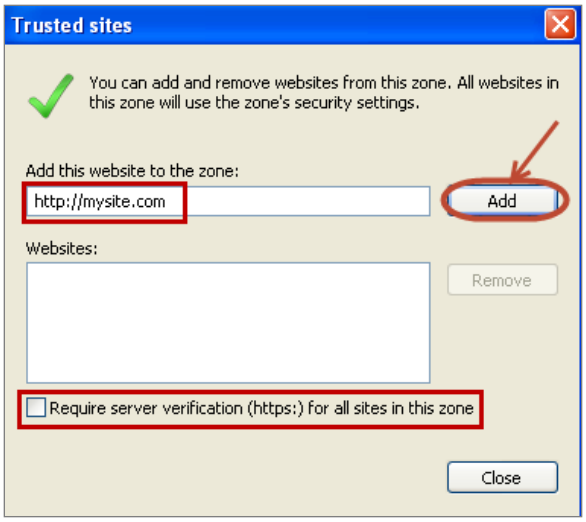
1. Browse to your Web Modules URL.
2. If prompted for a windows logon, enter your username and password to log on.
3. Open the Tools Menu and choose **Internet Options**. If you do not see the Tools menu, hold the ALT key to show the Tools menu.
4. Select the **Security** tab and click **Trusted sites** security zone.
5. Click the **Sites** button.



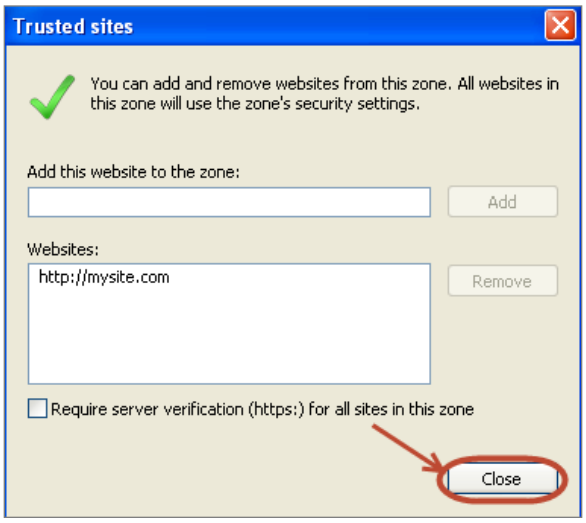

6. Un-check the box: Require server verification (https:) for all sites in this zone.
7. Verify the site in the Add this website to the zone: box. It should be the website that hosts the EAM Web Modules.

   Only the hostname or IP is required. For example, if the website URL is "http://mysite.com/mysite/default.aspx," then the website you add should be “http://mysite.com.”

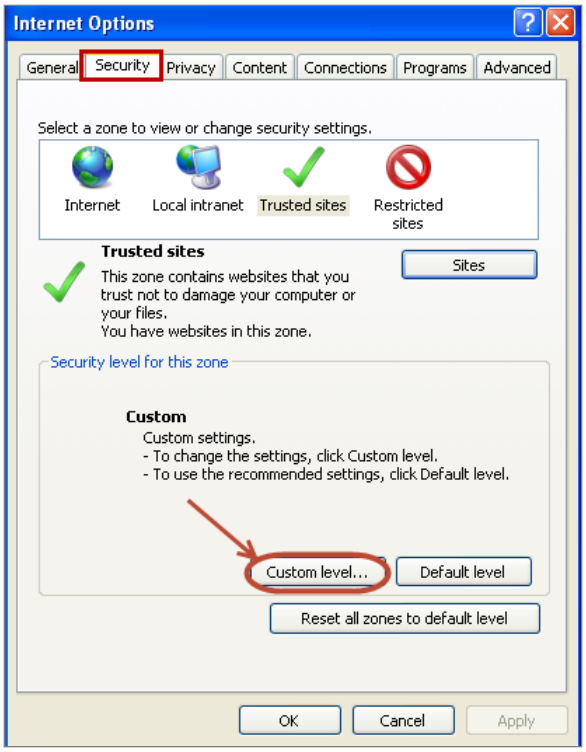
8. Click the **Add** button.




9. Click the **Close** button.

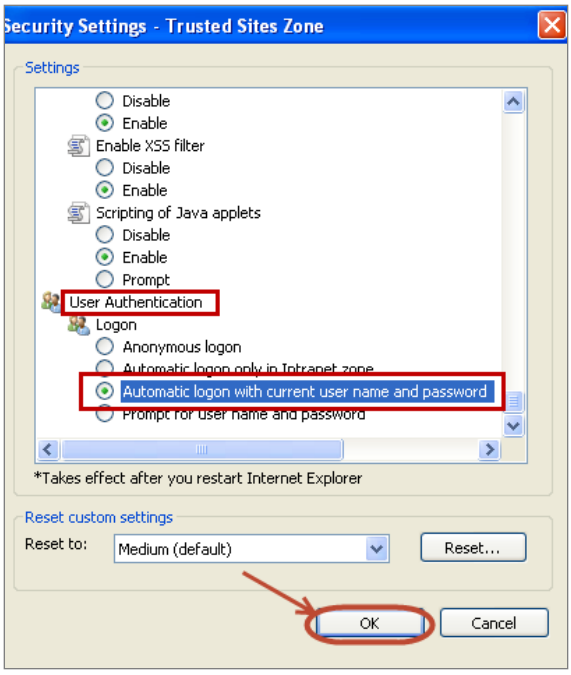



10. Back on the **Security** tab, click the **Custom level** button.

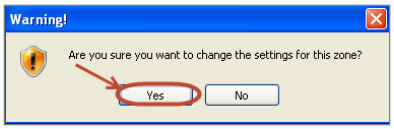



11. Scroll all the way down to find the User Authentication section and select the radio button for Automatic logon with current user name and password.

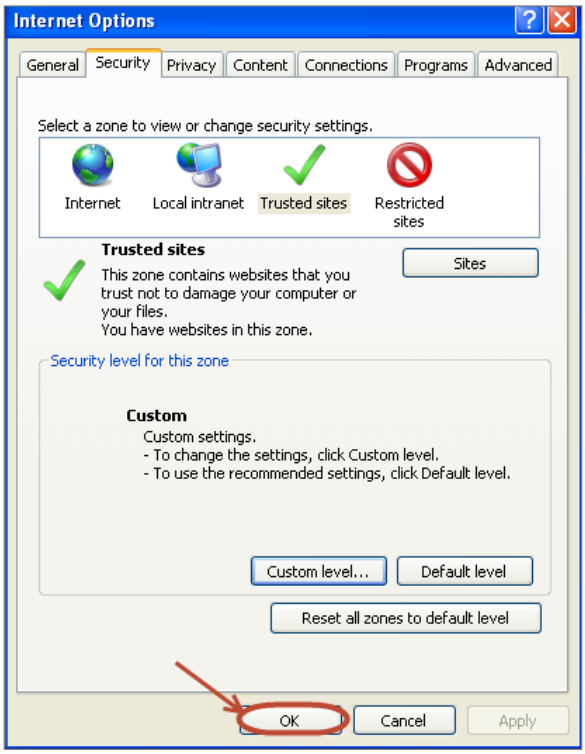
12. Click the OK button.




13. If prompted to change settings, click the **Yes** button.




14. Click the **OK** button to complete the browser configuration for Single Sign-On.




# Testing Automatic Single Sign-on

**To ensure automatic Single Sign-On works correctly:**

1. Close browser.
2. Reopen browser.
3. Navigate to the Web Modules URL.
4. When prompted, enter username and password, and check **Remember my password**.
5. Once successfully logged into the product, close Internet Explorer again.
6. Repeat steps 4-5. You should no longer be prompted to enter your saved password. If you are, there are likely other security settings in play.