



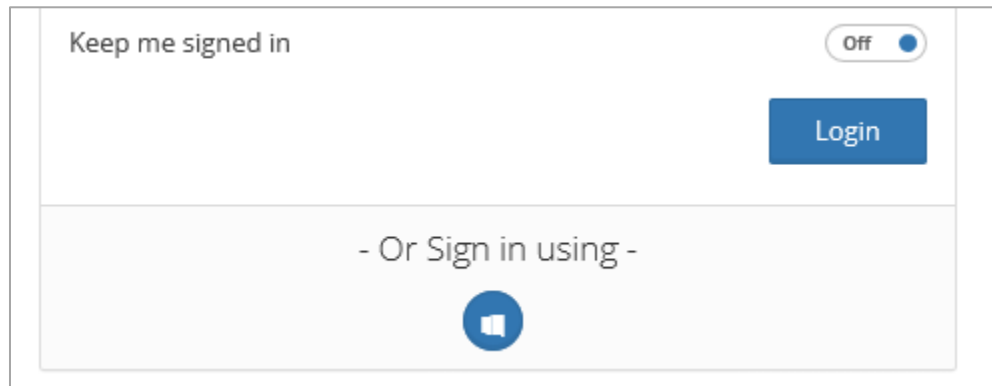
# ServicePRO Web

*ServicePRO Web AD Pass-through  
Authentication*

## Overview

This document outlines how to set up AD Pass-through Authentication for ServicePRO Web.

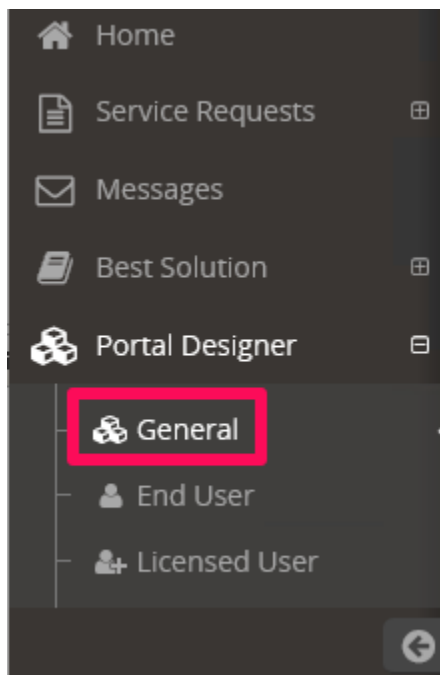
AD Pass-through Authentication in ServicePRO Web can be accessed from the Windows Login button, located at the bottom of the ServicePRO Web Login section.



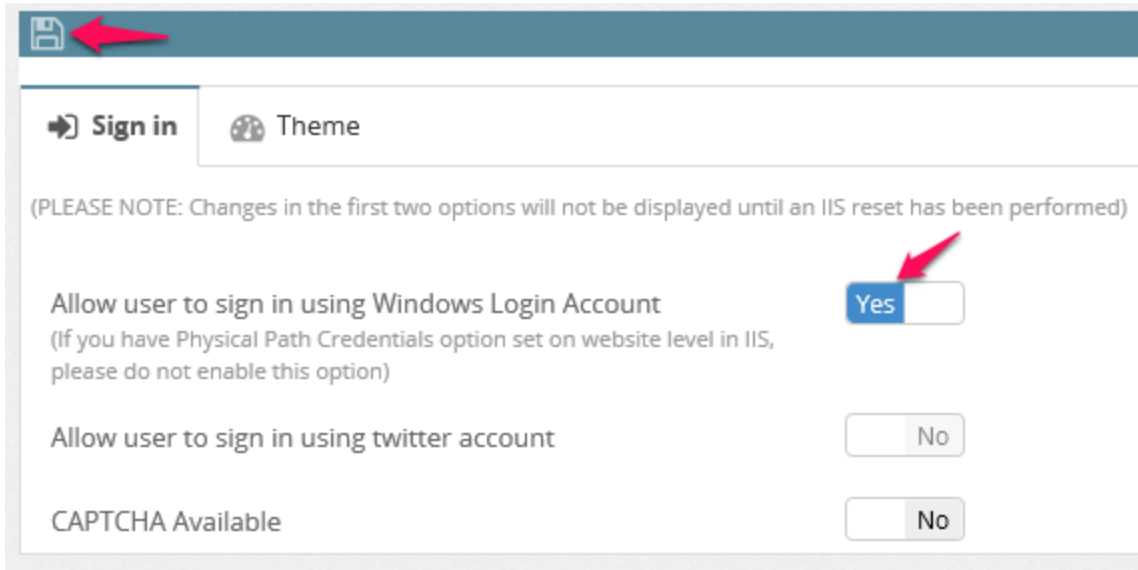
## Enabling Sign in using Windows Login Account

A ServicePRO Administrator will need to enable this feature before the option becomes available on the login screen.

- 1) Login to ServicePRO Web as a **ServicePRO Administrator**.
- 2) On the left panel, select **Portal Designer->General**, this will bring you to the 'Sign in' Tab.



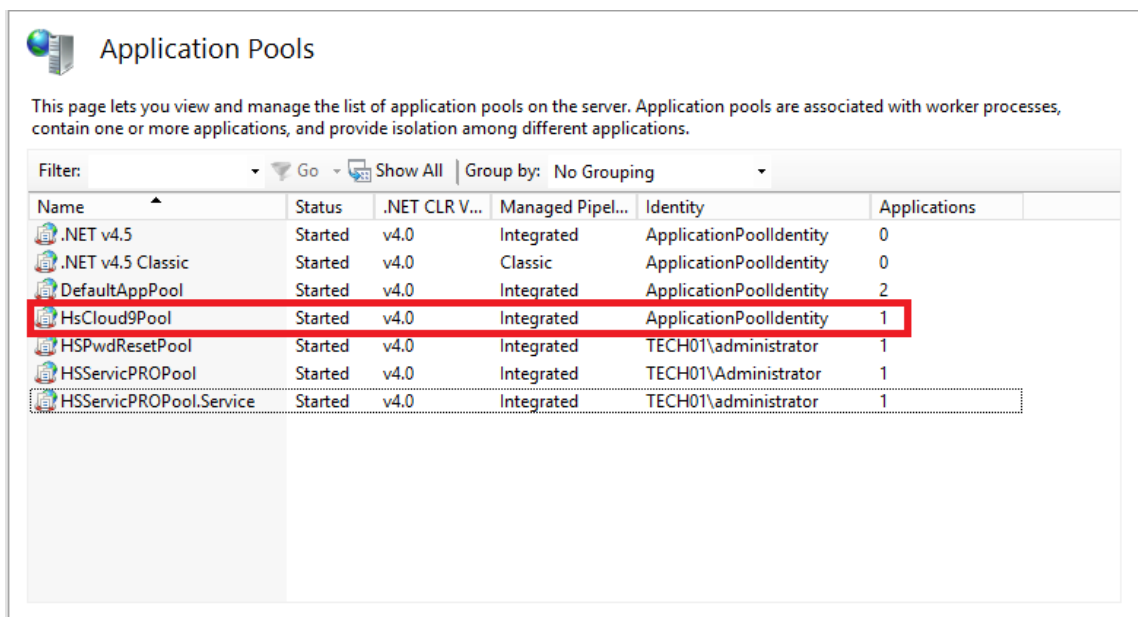
- 3) Change the value to **Yes** where it says **Allow user to sign in using Windows Login Account** and save the changes.



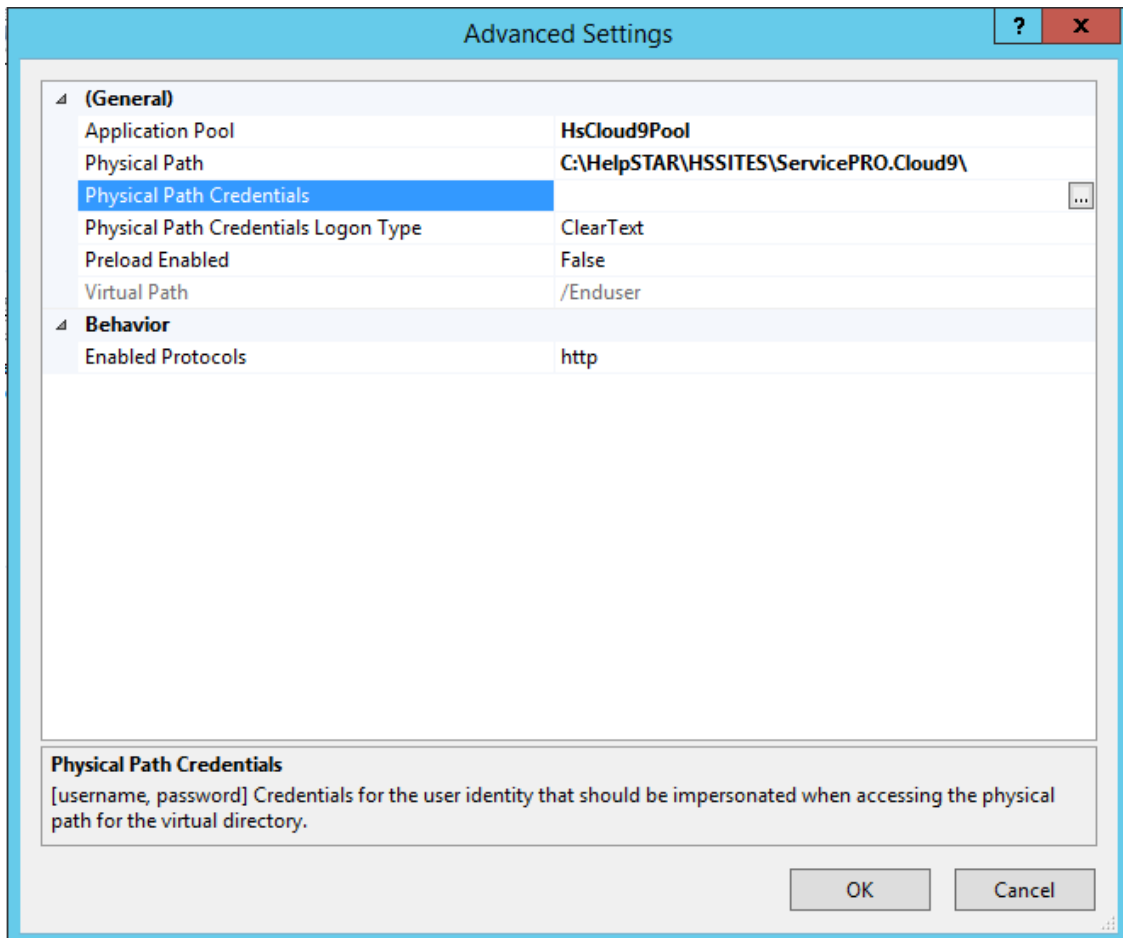
## Pre-requisite Settings on the Web Server

In order for ServicePRO ServicePRO Web AD pass through to work, the following settings need to be modified in the Web server where all the ServicePRO portals are installed.

- 1) Change the authentication **Identity** in the Application pool for ServicePRO ServicePRO Web **HsCloud9Pool** to **ApplicationPoolIdentity**.



- 2) In the Cloud Virtual Directory, make sure **Physical Path Credentials** are set to use Application User(pass-through authentication)



**Advanced Settings**

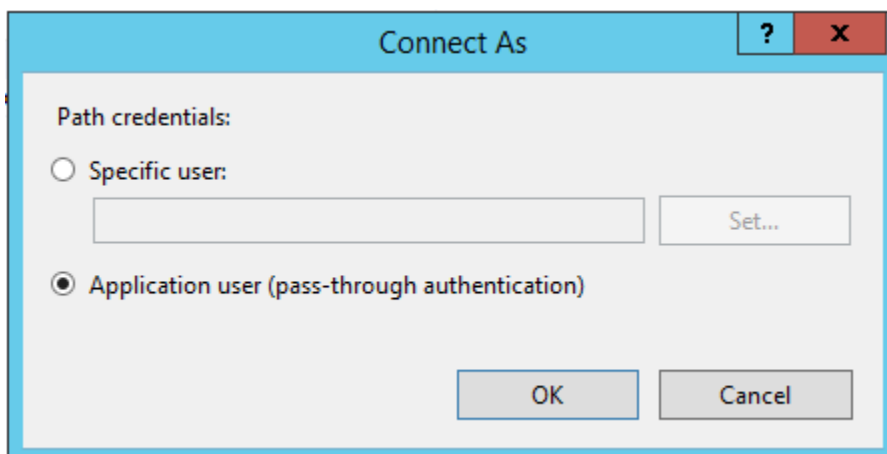
Application Pool	HsCloud9Pool
Physical Path	C:\HelpSTAR\HSSITES\ServicePRO.Cloud9\
<b>Physical Path Credentials</b>	...
Physical Path Credentials Logon Type	ClearText
Preload Enabled	False
Virtual Path	/Enduser

**Behavior**

Enabled Protocols	http
-------------------	------

**Physical Path Credentials**  
[username, password] Credentials for the user identity that should be impersonated when accessing the physical path for the virtual directory.

OK Cancel



**Connect As**

Path credentials:

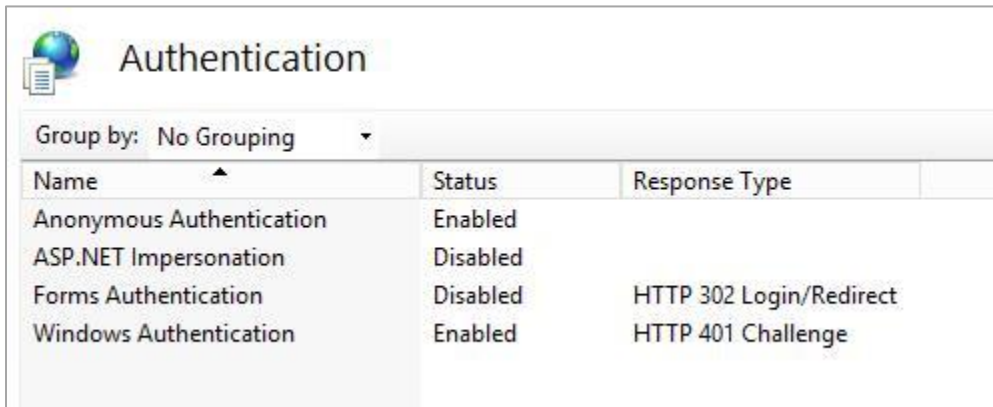
Specific user:

Set...

Application user (pass-through authentication)

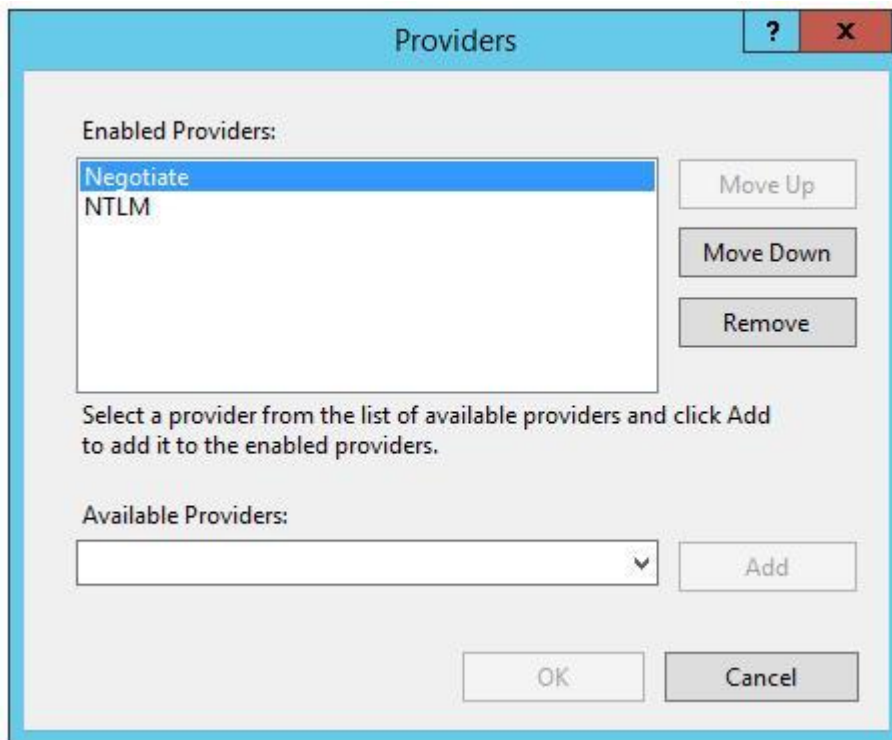
OK Cancel

- 3) On the ServicePRO Web Virtual Directory, both **Anonymous** and **Windows Authentication** should be enabled. **Form Authentication** is not supported and therefore should be disabled.



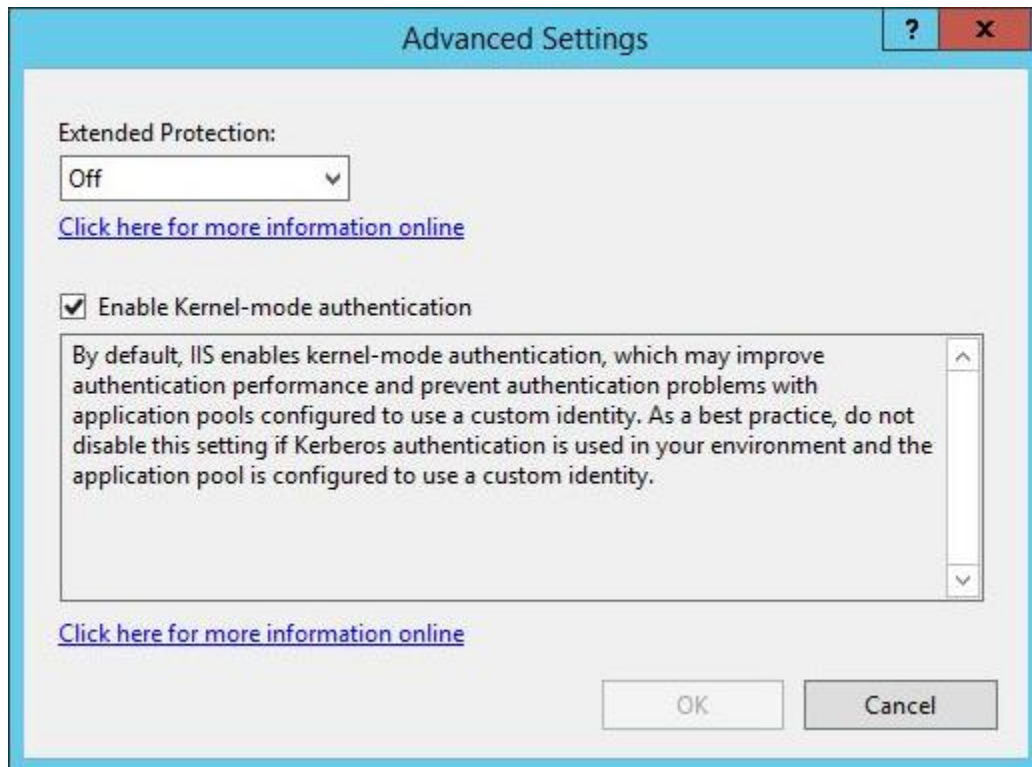
Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

- 4) Next, for **Windows Authentication**, **Negotiate** should be moved to top of the Enabled Providers listing, rather than **NTLM**. The providers should already be arranged in this order by default unless it was changed manually.



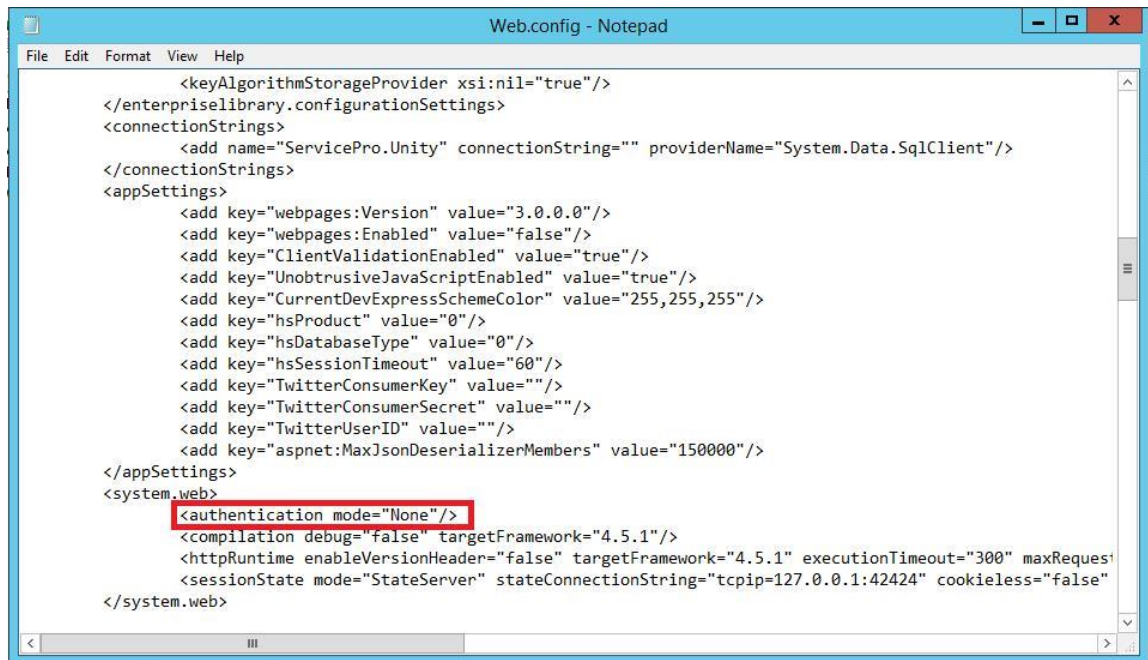
5) Under Advanced Settings for Windows Authentication, ensure settings appear as shown below.

- **Extended Protection:** Off
- **Enable Kernel-mode authentication:** On



- 6) Finally, change the Authentication to “None” on ServicePRO Web Web.config located at:  
C:\HelpSTAR\HSSITES\ServicePRO.ServicePRO Web\Web.config

Please create a backup of the Web.config file before making any changes.



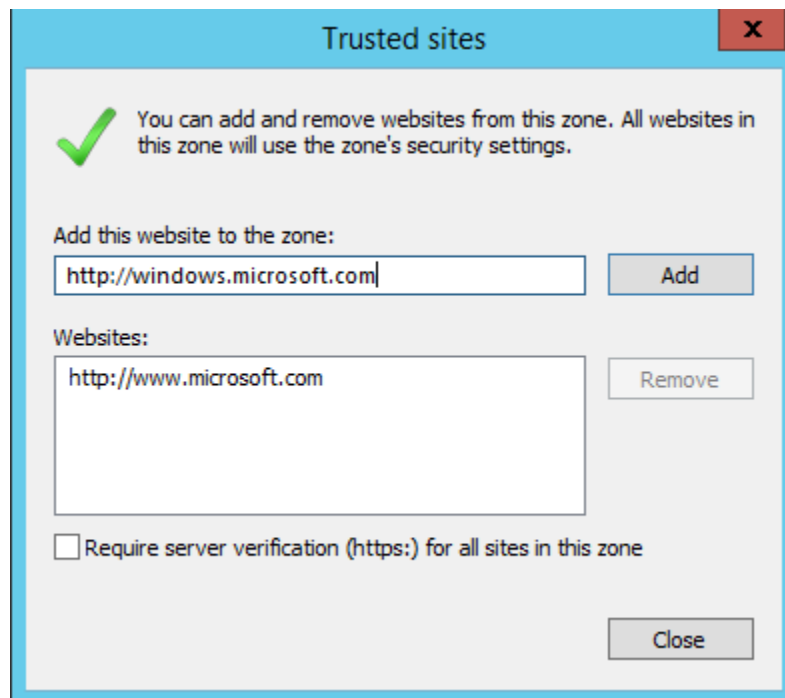
```
Web.config - Notepad
File Edit Format View Help
<keyAlgorithmStorageProvider xsi:nil="true"/>
</enterpriselibrary.configurationSettings>
<connectionStrings>
  <add name="ServicePro.Unity" connectionString="" providerName="System.Data.SqlClient"/>
</connectionStrings>
<appSettings>
  <add key="webpages:Version" value="3.0.0.0"/>
  <add key="webpages:Enabled" value="false"/>
  <add key="ClientValidationEnabled" value="true"/>
  <add key="UnobtrusiveJavaScriptEnabled" value="true"/>
  <add key="CurrentDevExpressSchemeColor" value="255,255,255"/>
  <add key="hsProduct" value="0"/>
  <add key="hsDatabaseType" value="0"/>
  <add key="hsSessionTimeout" value="60"/>
  <add key="TwitterConsumerKey" value="" />
  <add key="TwitterConsumerSecret" value="" />
  <add key="TwitterUserID" value="" />
  <add key="aspnet:MaxJsonDeserializerMembers" value="150000"/>
</appSettings>
<system.web>
  <authentication mode="None"/>
  <compilation debug="false" targetFramework="4.5.1"/>
  <httpRuntime enableVersionHeader="false" targetFramework="4.5.1" executionTimeout="300" maxRequest
  <sessionState mode="StateServer" stateConnectionString="tcpip=127.0.0.1:42424" cookieless="false"
</system.web>
```

- 7) After making all changes listed, please reset the IIS by running **IISRESET** from within the IIS Manager or from a command prompt by running the command: iisreset.

## Pre-requisite Settings on the Client System

In order for the browser to pass the Windows user credentials for the user currently logged in, the following settings should be adjusted:

1. Under in your browser's Internet options, navigate to: **Tools > Internet Options > Security (tab)** and select **Trusted Sites** then click on **Sites**. Add the website for ServicePRO Web to your Trusted Sites list. If you are not using SSL (HTTPS), you will have to uncheck the option to "Require server verification (https:) for all sites in this zone" before clicking on Add.



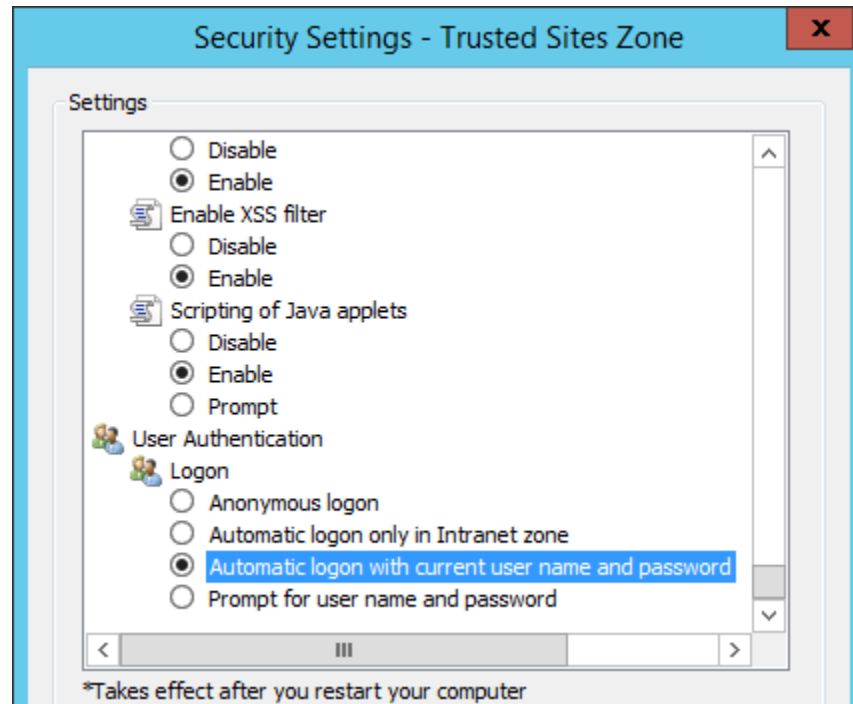


2. Next select **Custom Level**

This will open the Security Settings – Trusted Sites Zone window.

From here, navigate to the **User Authentication – Logon** section.

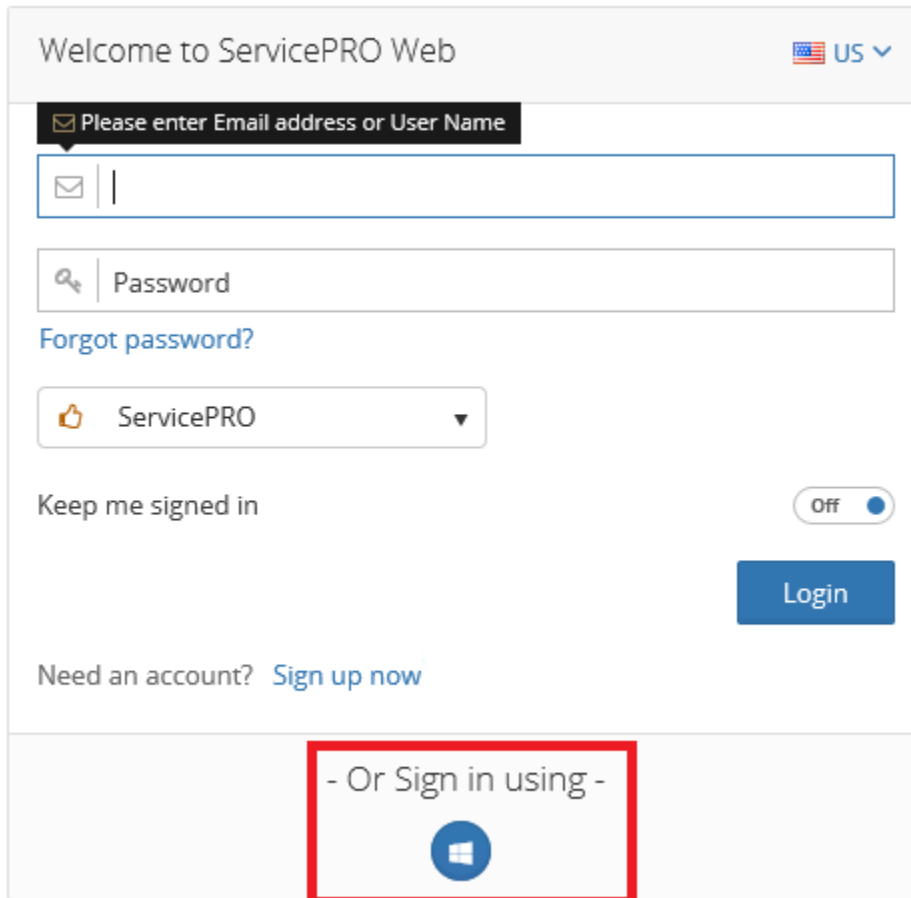
Enable **Automatic logon with current user name and password**.



**Note:** Depending on the security within the browser, if these settings are not set correctly then you might be prompted for your Windows credentials before it will pass you through. You may also need to contact your Administrator if these settings are greyed out as they would be controlled through Group Policy. Some browsers like Mozilla Firefox do not support Automatic Logon so it will always prompt you for credentials.

## How Pass-through Authentication Works

For the first time, the user will need to click on the **Windows Login** button in order to log in (highlighted with a red rectangle in the picture below). This is similar to the **Continue** button in ServicePRO.



If the user exits ServicePRO Web by closing the browser (i.e. exits without using the Sign Out option), then the user will be directly taken back to the respective page without prompting for login whenever they visit the ServicePRO Web URL, the ServicePRO Web Approval Link, the Suggested Link URL or the Request URL (i.e. Pass-through Authentication will occur).

If the user exits ServicePRO Web using the **Sign Out** option, the Pass-through Authentication will not work. The user will need to click on the **Windows Login** button again.