

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.

Sign in	🚯 Theme				
(PLEASE NOTE: Changes in the first two options will not be displayed until an IIS reset has been performed)					
(If you have Ph	o sign in using Windows Login Account nysical Path Credentials option set on website level in IIS, enable this option)	Yes			
Allow user to	o sign in using twitter account	No			
CAPTCHA AV	vailable	No			

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.**

		· ·	oup by: No Groupi	ng •	
lame 🗖	Status	.NET CLR V	Managed Pipel	Identity	Applications
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolIdentity	0
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolIdentity	0
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolIdentity	2
HsCloud9Pool	Started	v4.0	Integrated	ApplicationPoolIdentity	1
JHSPwdResetPool	Started	v4.0	Integrated	TECH01\administrator	1
HSServicPROPool	Started	v4.0	Integrated	TECH01\Administrator	1
HSServicPROPool.Service	Started	v4.0	Integrated	TECH01\administrator	1



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

	Advanc	ed Settings		?	x
✓ (Genera Applicat	ion Pool	HsCloud9Pool	San daa BBO (laado)		
Physical		C:\HelpSTAR\HSSITES\	ServicePKO.Cloud9\		
	Path Credentials	Chartert			
	Path Credentials Logon Type	ClearText			
Preload I Virtual P		False			_
		/Enduser			
⊿ Behavio	r Protocols	http			
[username, p	h Credentials password] Credentials for the user identity t virtual directory.	hat should be impersonate	ed when accessing the p	ohysica	
				cunc	- -
	Connect As	?	×		
Path crede	entials:				
O Specifi	c user:				
		Set			
Application	ation user (pass-through authenticat	ion)			
	C	K Cance	el		



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.

Authentication		
Group by: No Grouping 🔹		
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.

Negotiate NTLM		Move Up
		Move Down
		Remove
	m the list of available providers	and click Add
Select a provider from to add it to the enab Available Providers:		and click Add



- 5) Under Advanced Settings for Windows Authentication, ensure settings appear as shown below.
 - Extended Protection: Off
 - Enable Kernel-mode authentication: On

1:				
~				
information online				
bles kernel-mode a formance and prev configured to use a j if Kerberos auther	uthentication, w vent authenticat custom identit itication is used	ion problems wi y. As a best prac in your environ	ith tice, do not	<
information online	2			
		ОК	Cancel	-
	node authentication oles kernel-mode a formance and prev configured to use a if Kerberos auther configured to use	formance and prevent authenticat configured to use a custom identity if Kerberos authentication is used	node authentication oles kernel-mode authentication, which may impro formance and prevent authentication problems wi configured to use a custom identity. As a best prac if Kerberos authentication is used in your environ configured to use a custom identity.	node authentication bles kernel-mode authentication, which may improve formance and prevent authentication problems with configured to use a custom identity. As a best practice, do not if Kerberos authentication is used in your environment and the configured to use a custom identity.



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	x
File	Edit	Format View Help	
		<keyalgorithmstorageprovider xsi:nil="true"></keyalgorithmstorageprovider>	1
		<connectionstrings></connectionstrings>	
		<pre><add connectionstring="" name="ServicePro.Unity" providername="System.Data.SqlClient"></add></pre>	
		<appsettings></appsettings>	
		<add key="webpages:Version" value="3.0.0.0"></add>	
		<add key="webpages:Enabled" value="false"></add>	
		<add key="ClientValidationEnabled" value="true"></add>	-
		<add key="UnobtrusiveJavaScriptEnabled" value="true"></add>	-
		<add key="CurrentDevExpressSchemeColor" value="255,255,255"></add>	- 14
		<add key="hsProduct" value="0"></add>	
		<add key="hsDatabaseType" value="0"></add>	
		<add key="hsSessionTimeout" value="60"></add>	
		<add key="TwitterConsumerKey" value=""></add>	
		<add key="TwitterConsumerSecret" value=""></add>	
		<add key="TwitterUserID" value=""></add>	
		<add key="aspnet:MaxJsonDeserializerMembers" value="150000"></add>	
		<system.web></system.web>	
		<pre><authentication mode="None"></authentication></pre>	
		<compilation debug="false" targetframework="4.5.1"></compilation>	
		<pre><httpruntime enableversionheader="false" executiontimeout="300" maxreque<="" pre="" targetframework="4.5.1"></httpruntime></pre>	st
		<pre></pre>	

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:

 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.

Trusted sites	×			
You can add and remove websites from this zon this zone will use the zone's security settings.	e. All websites in			
Add this website to the zone:				
http://windows.microsoft.com	Add			
Websites:				
http://www.microsoft.com	Remove			
Require server verification (https:) for all sites in this zone				
	Close			



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.

Security Settings - Trusted Sites Zone	
Settings	
O Disable	
Enable	
Enable XSS filter	
O Disable	
Enable	
Scripting of Java applets	
O Disable	
Enable	
O Prompt	
A User Authentication	
& Logon	
O Anonymous logon	
 Automatic logon only in Intranet zone 	
Automatic logon with current user name and password	
Prompt for user name and password	-
	Ľ
*Takes effect after you restart your computer	

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.

Welcome to Service	PRO Web	🔤 US 🗸
Please enter Email add	ress or User Name	
Revealed Password		
Forgot password?		
🖒 ServicePRO	•	
Keep me signed in		Off ●
		Login
Need an account? Sign	n up now	
	- Or Sign in using -	
	•	

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.