SERVICEPRO Cloud9

Cloud9 AD Pass-through Authentication

Overview

This document outlines how to set up AD Pass-through Authentication for Cloud9.

AD Pass-through Authentication in Cloud9 can be accessed from the Windows Login button, located at the bottom of the Cloud9 Login section.

# Pre-requisite Settings on the Web Server

In order for ServicePRO Cloud9 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 Cloud9 **HSCloud9Pool** to **ApplicationPoolIdentity.**
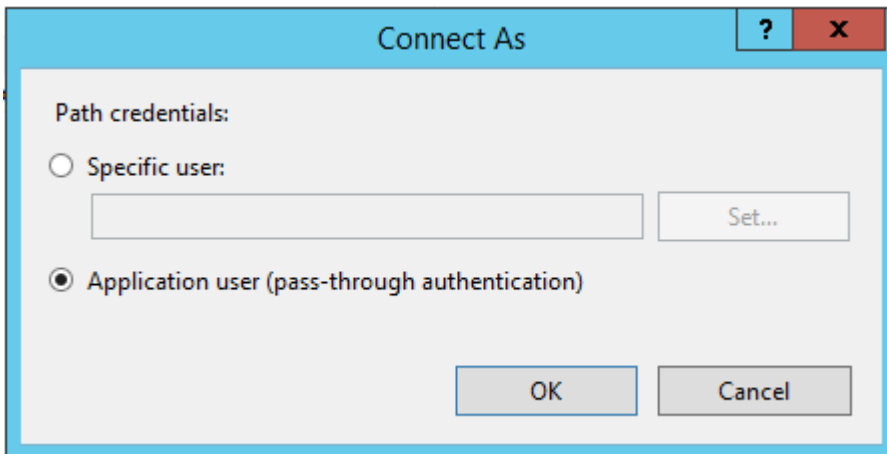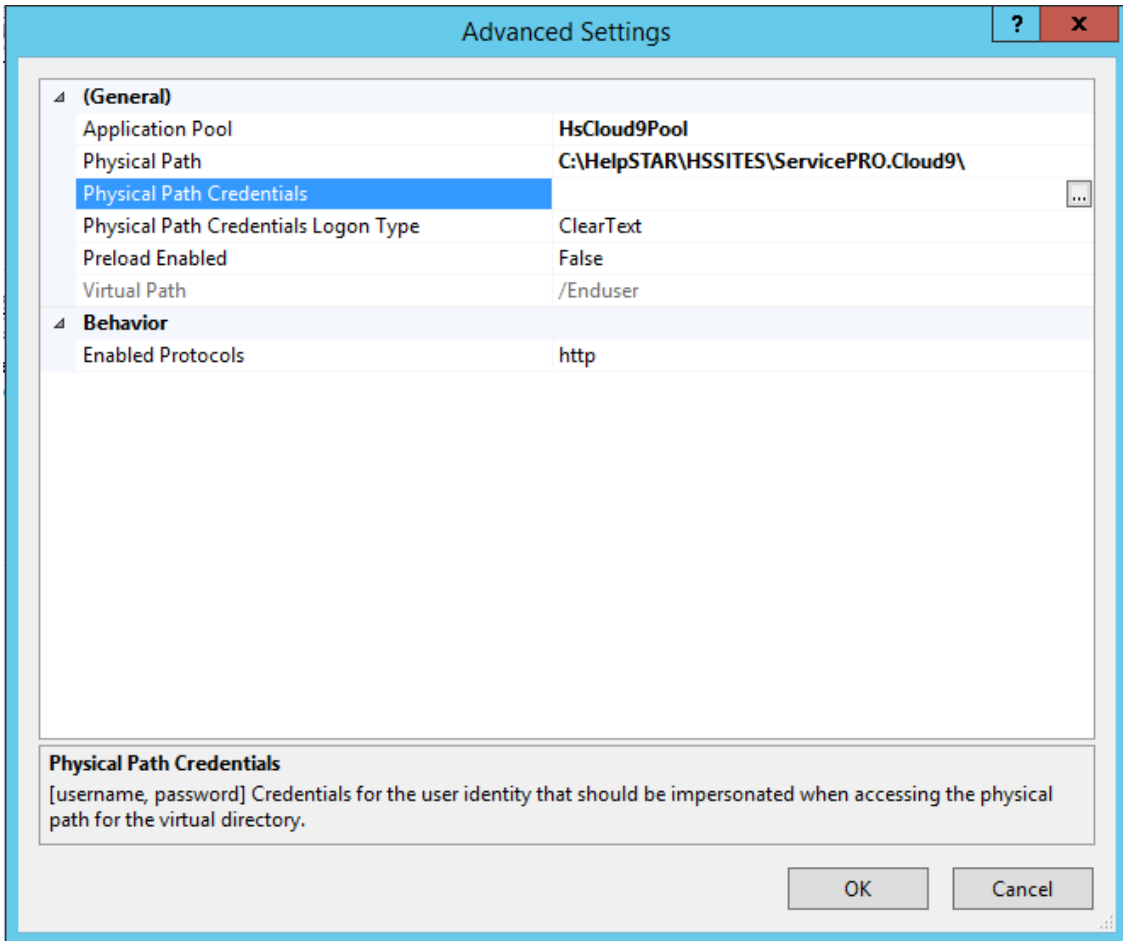

---

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

3) On the Cloud9 Virtual Directory, both **Anonymous** and **Windows Authentication** should be enabled. **Form Authentication** is not supported and therefore should be disabled.

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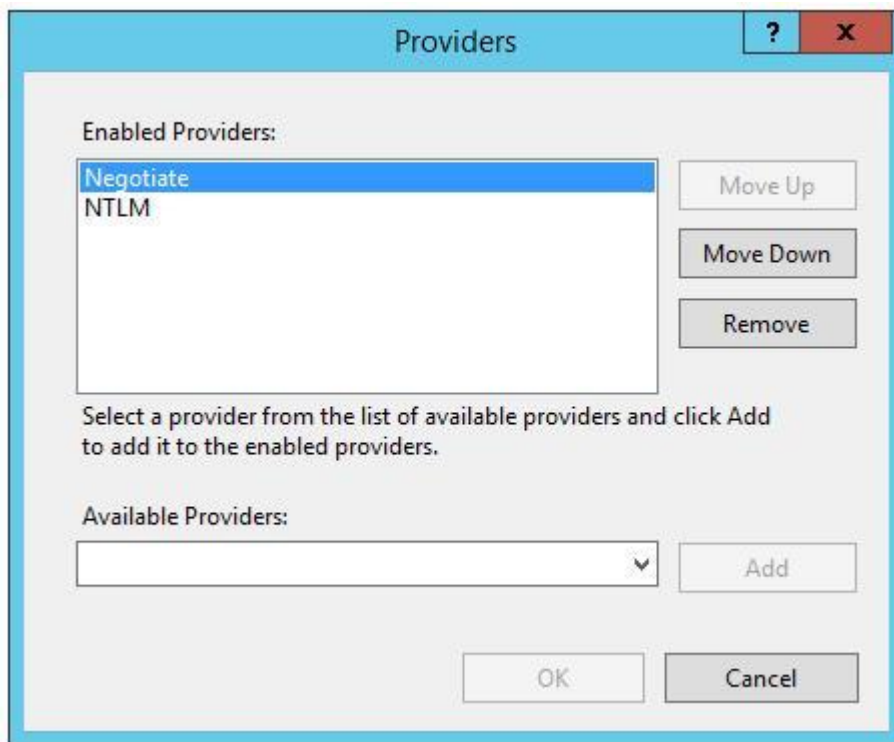
5) Under Advanced Settings for Windows Authentication, ensure settings appear as shown below.

- **Extended Protection**: Off

- **Enable Kernel-mode authentication**: On
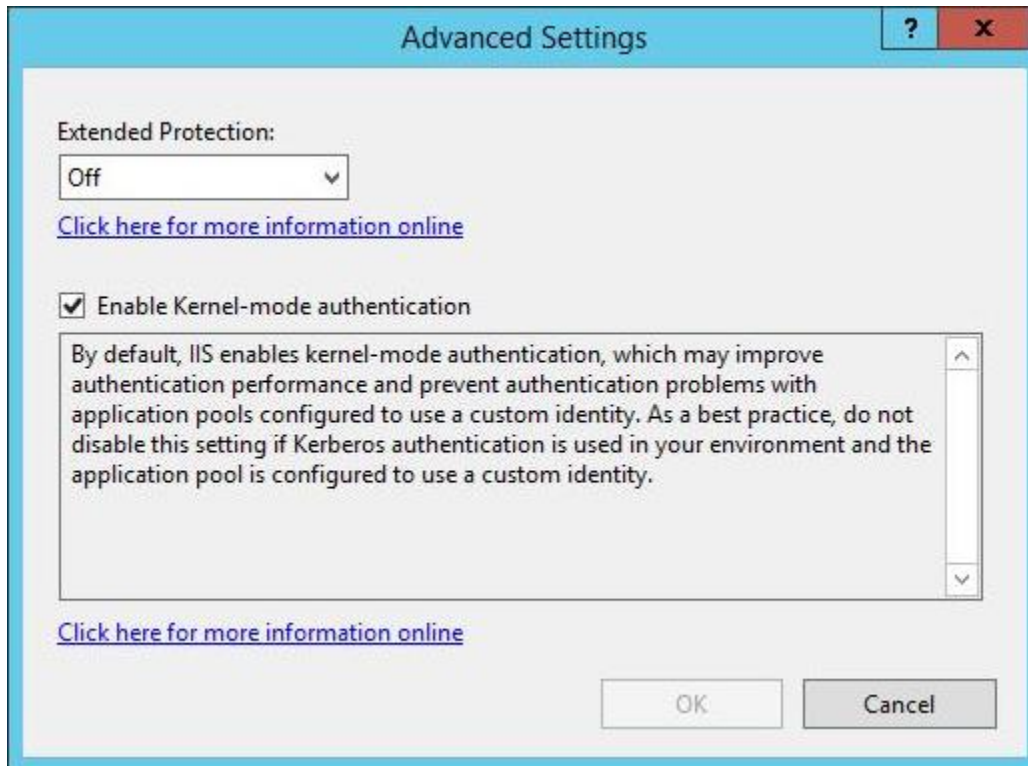
6) Finally, change the Authentication to "**None**" on Cloud9 Web.config located at:

    `T:\HelpSTAR\HSSITES/ServicePRO.Cloud9/Web.config`

    (Where T: is the mapped drive for the HelpSTAR network installation)
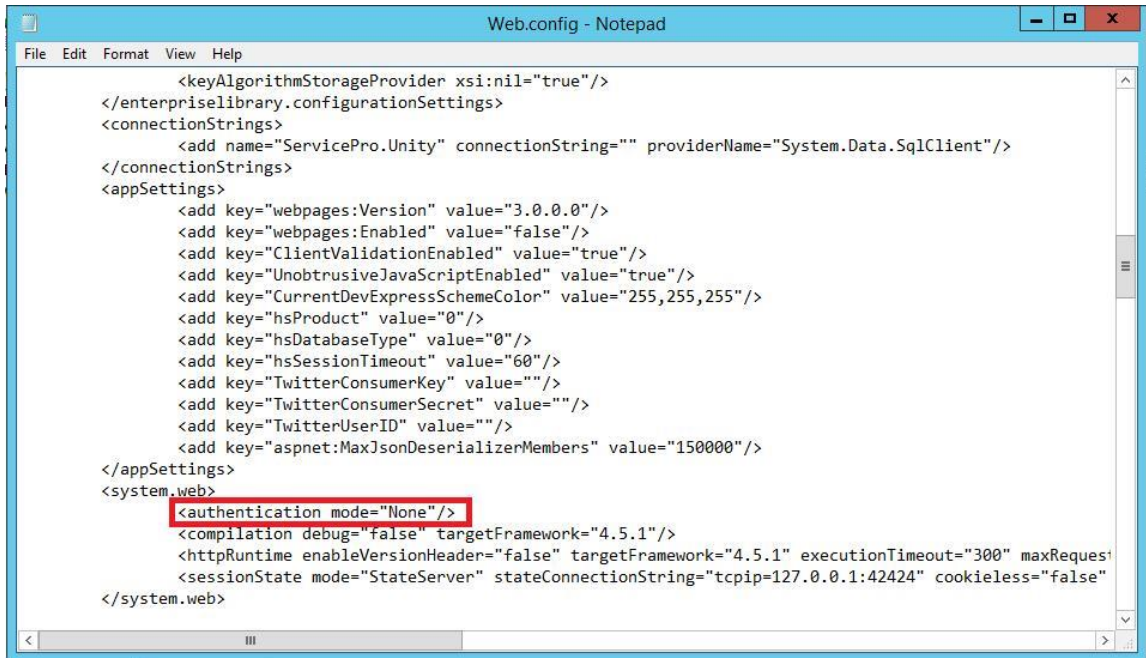
    Please create a backup of the Web.config file before making any changes.

7) After making all changes listed, please reset the IIS by running **IISRESET** from the command prompt.

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) > Custom Level
   This will open the Security Settings – Internet Zone window.

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

   Enable **Automatic logon with current user name and password**.
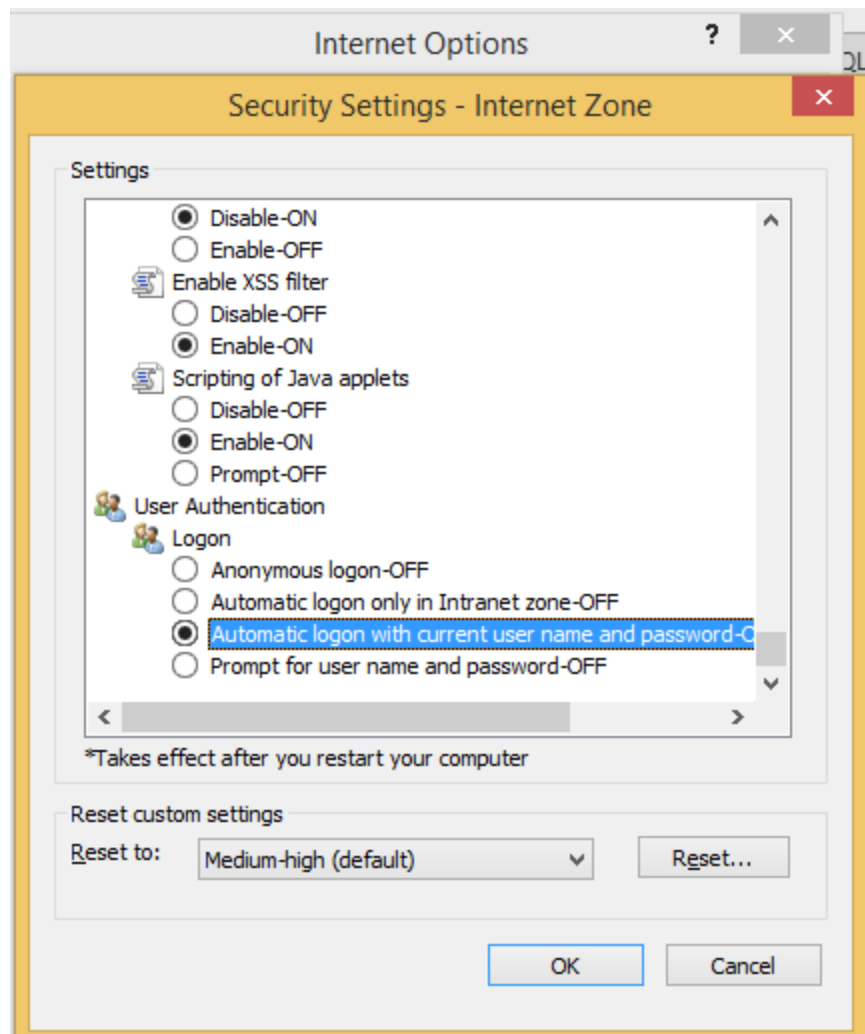
2. Add the website for Cloud9 to your Trusted Sites list, also under the **Security** tab.
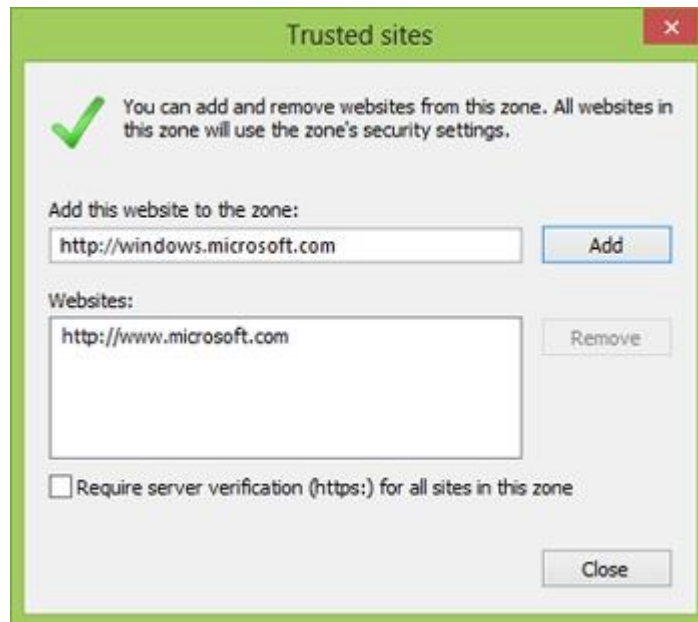
3. When the user clicks on **Windows Login** button in Cloud9 for the very first time, the user will be prompted to enter Windows Security credentials.
   When prompted, after entering the credentials, the user should ensure to check off the **Remember my credentials** check box.

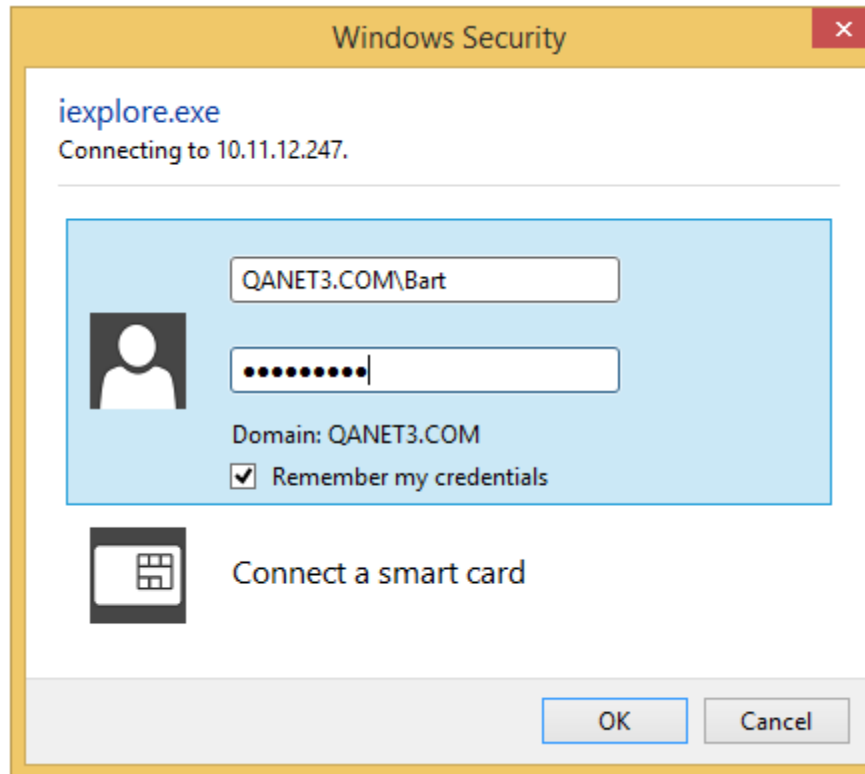**NOTE**: If the **Remember my credentials** checkbox is selected, the user will not be prompted with this dialog again the next time they log in with the Windows Login button.

If the setting mentioned in step 1 was not enabled, the Remember my credentials check box will not be visible. The user needs to update the setting mentioned in step 1 first.
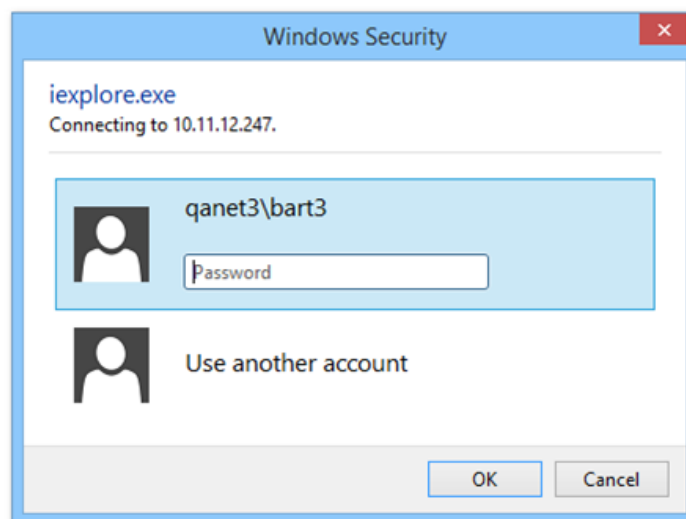
How Pass-through Authentication Works

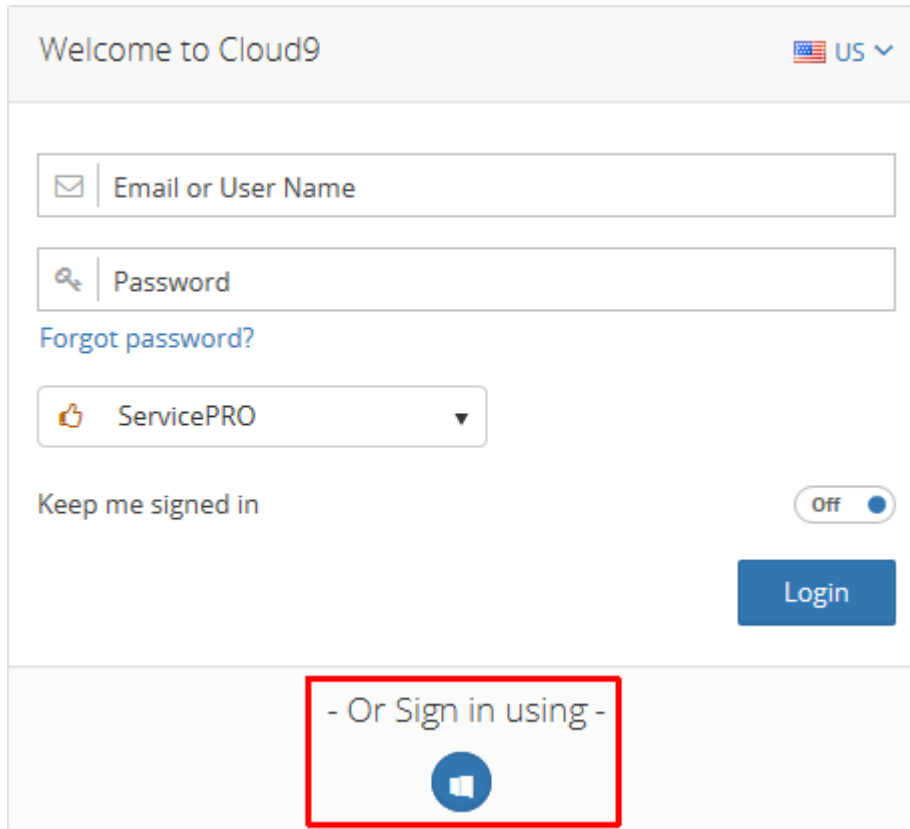For the first time, the user will need to click on the **Windows Login** button in order to log in (highlighted with a red rectangle in the picture below). This is similar to the **Continue** button in ServicePRO.

If the user exits Cloud9 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 Cloud9 URL, the Cloud9 Approval Link, the Suggested Link URL or the Request URL (i.e. Pass-through Authentication will occur).

If the user exits Cloud9 using the **Sign Out** option, the Pass-through Authentication will not work. The user will need to click on the **Windows Login** button again.