Active Directory Authentication:

Employees generally log in to Self Service using a standard username and password native to the software. These logins can also be configured to connect with Windows Active Directory. This means that employees will be immediately logged into their profile as soon as they navigate to the Self Service portal, based on the Windows Credentials they are logged into their computer as.

Please note that because employees do not need a separate login, they must take reasonable precaution to prevent unauthorised access to their computers. If they leave their computers unattended there is nothing stopping another employee using Self Service and getting access to their details. Employees must log out of Windows or lock their computer, requiring a Windows username and password to be entered to unlock it.

Using Windows authentication also means that in order for an employee to view their own details on a computer other than their own, they must first log the current user out of Windows and login as themselves. They can't just log out of the Self Service module and back in as themselves.

Please Note: Do not setup Windows Authentication for the user who will be accessing Self Service as the ADMIN user. They will not be able to log out in order to log in as Admin if this has been setup on their PC.

IIS will need to be configured so that **Anonymous Authentication** is switched **off** and **Windows Authentication** is switched **on**.

IIS v6.0 or below:

Run IIS, right-click the SimplyWebPersonnel site and view the **Properties**. Select the **Directory Security** tab and then by click on the **Edit** button. Make sure **Enable anonymous access** is not selected but the **Integrated Windows authentication** option is.

IIS v7.0 or above:

Run IIS and left-click the SimplyWebPersonnel site in the left-hand pane. Double-click the **Authentication** icon in the middle pane. Right-click the **Anonymous Authentication** option from the list and select **Disable**. Now right-click the **Windows Authentication** option and click **Enable**.

The web.config must also be modified to enable **Identity Impersonation** for the SQL Server connection. Open the **C:\Inetpub\wwwroot\SimplyWebPersonnel\web.config** file in Notepad and locate the line below:

```
<identity impersonate="true"/>
```

This will need to be changed to specify the domain, username and password of the Windows user to authenticate, which should generally be a dedicated domain service account:

```
<identity impersonate="true" userName="OurDomain\Svc_SelfService"
password="8gsU$ltt"/>
```

Please note that **the username and password will be visible in plain text** unless you follow the instructions in the following Microsoft article:

. NET V4 - https://msdn.microsoft.com/en-us/library/72wdk8cc%28v=vs.100%29.aspx

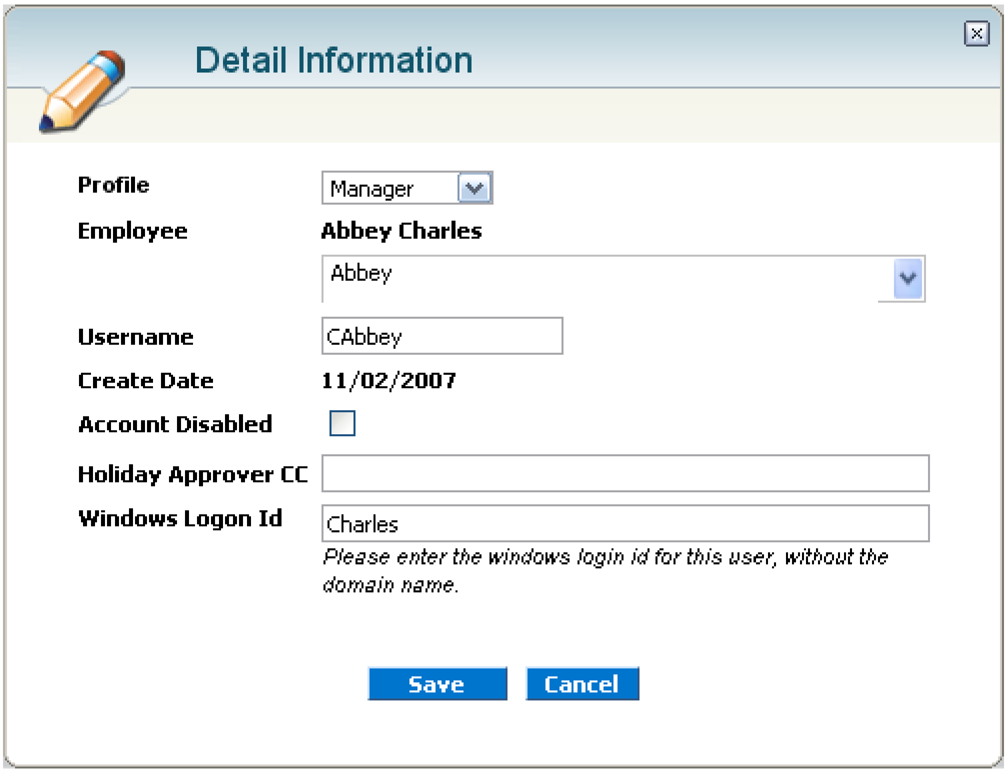
.NET V3 - https://msdn.microsoft.com/en-us/library/72wdk8cc%28v=vs.85%29.aspx

.NET V2 - https://msdn.microsoft.com/en-us/library/72wdk8cc%28v=vs.80%29.aspx

This article will explain how to encrypt the username and password into the server's registry.

Once the web site has been set to use Windows Authentication, the final step is to link each Self Service login to its respective Windows username from your Active Directory system. To do this, log in to the Self Service module as the **ADMIN** user and select **System Setup > Users**. Click on the **green pencil icon** next to the user you wish to update.

The Username shown here will not be used but the Self Service module requires a unique username for every employee to be entered. The field that needs to be completed to use Windows Authentication is the **Windows Logon Id** field.



Profile	Manager
Employee	Abbey Charles Abbey
Username	CAbbey
Create Date	11/02/2007
Account Disabled	□
Holiday Approver CC	
Windows Logon Id	Charles *Please enter the windows login id for this user, without the domain name.*

The **Windows Logon Id** field must be set to the employee's Windows username **exactly as it appears in Active Directory** but without the prefixed domain name. For example, if the user logs on to the "**OurDomain**" domain as the user "**JoeBloggs**" then the value entered must be "**JoeBloggs**" and not the qualified name "**OurDomain\JoeBloggs**".

Once all of the details have been entered, click on the **Save** button and that user will be able to use the Self Service module without logging in.

If the user has previously logged in using a separate username and password and clicked on the "**Remember Me**" option on the login screen, please ask them to click on the "**Forget Me**" option or clear their web browser cookies **before** enabling the link to Active Directory.