

Ascentis HR Self-Service Setup and Security Guide



Introduction

You can rapidly set up Ascentis HR Self-Service and secure your IIS (Internet Information Services) web server in a short amount of time as follows:

STEP 1: Check that you have the prerequisites installed.

STEP 2: Check Windows Update for service packs and hot fixes. Allow it to install the Windows Automatic Updating feature.

STEP 3: Run the Self-Service setup program

STEP 4: Run additional configuration changes within IIS.

STEP 5: Configure SSL on your Web Server

Each step is described in detail on the following pages. By following these suggestions and instructions for installation, your Self-Service installation will be successful and your web server will be protected by multiple levels of security.

STEP 1: Prerequisites

Ascentis HR Self-Service setup must be applied on a machine running Windows Server 2003 or 2008 with IIS (Internet Information Server) 6.0 or later, .NET 3.5 Framework, and ASP.NET AJAX Extensions 1.0.

A SSL certificate is required for Ascentis Payroll users, while optional for all other users.

Note: If you install IIS AFTER the .NET Framework, see Microsoft article Q306005 at <http://support.microsoft.com/default.aspx?scid=KB;EN-US;q306005&>.

STEP 2: Create the Data Source

Note: This step can be skipped by Ascentis Payroll Users. Proceed to Step 3.

Before you run the Ascentis HR Self-Service setup program, you must first decide whether you want to make the application available to users from outside your company's internal, corporate network or whether it will also be available outside the network.

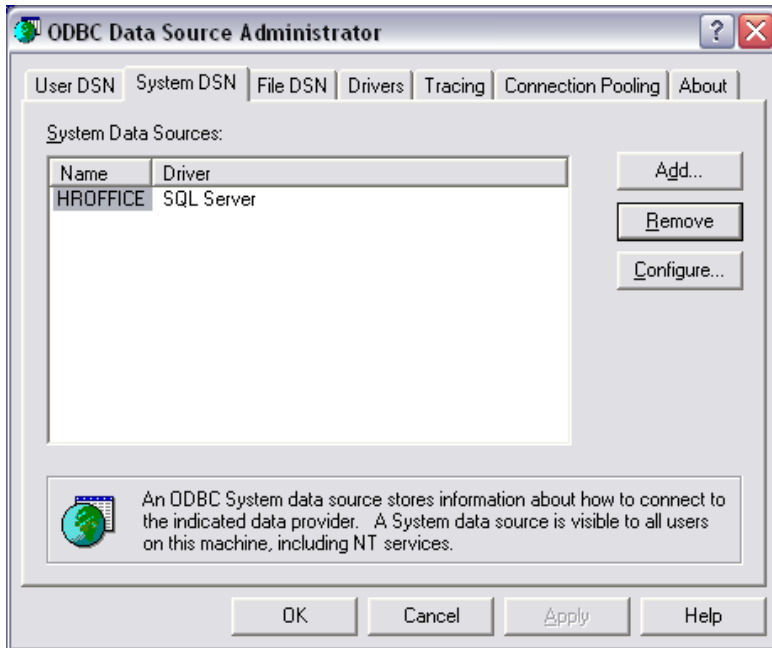
If you wish to make Ascentis HR Self-Service available only to users with access to your company's internal, corporate network you can simply run the Ascentis HR Client Setup on the web-server on your intranet that will house the Ascentis HR Self-Service application, and then proceed to STEP 3. See the Getting Started Guide for more information on running the Ascentis HR Client Setup.

Note: Running the Ascentis HR Client Setup on the web-server that will house the Ascentis HR Self-Service application, on your internal corporate network, is the preferred method for creating the DSN when you do not want to make Ascentis HR Self-Service available remotely via the Internet. The rest of

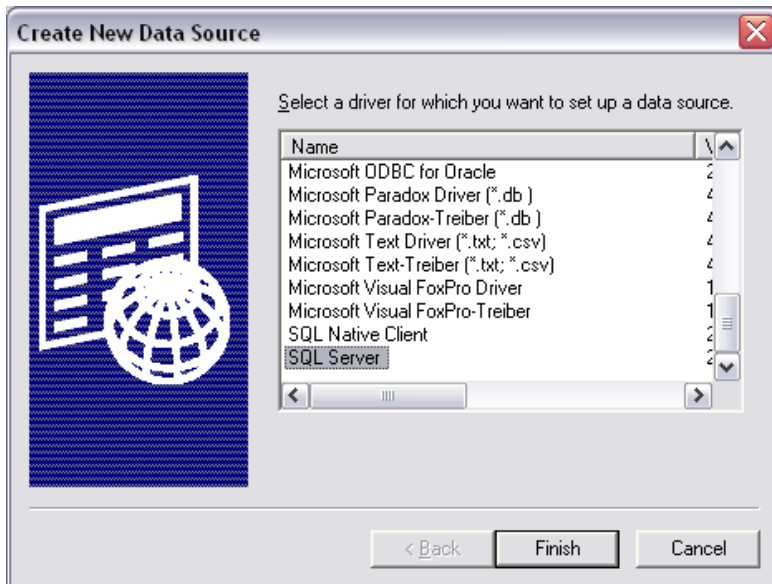
STEP 2 below only applies in situations where you have a firewall between your Internet web-server and your SQL Server and therefore cannot run the Ascentis HR Client Setup to create the Data Source.

In order to make Ascentis HR Self-Service available to users remotely via the Internet, you will first need to manually create a system Data Source Name (DSN) that will allow Ascentis HR Self-Service to communicate with the Ascentis HR database.

To create the System DSN manually, click on Start > Run. Type in "odbcad32" and press the OK button.

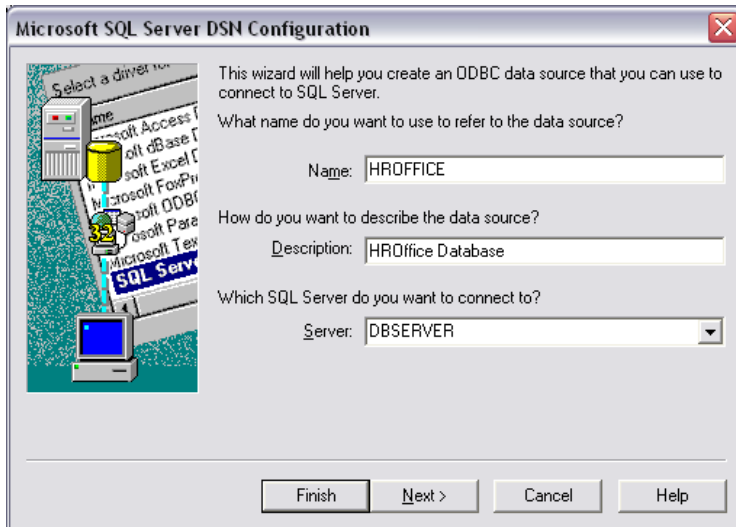


Select the *System DSN* tab, and then click **Add...** to open the *Create a New Data Source* window.

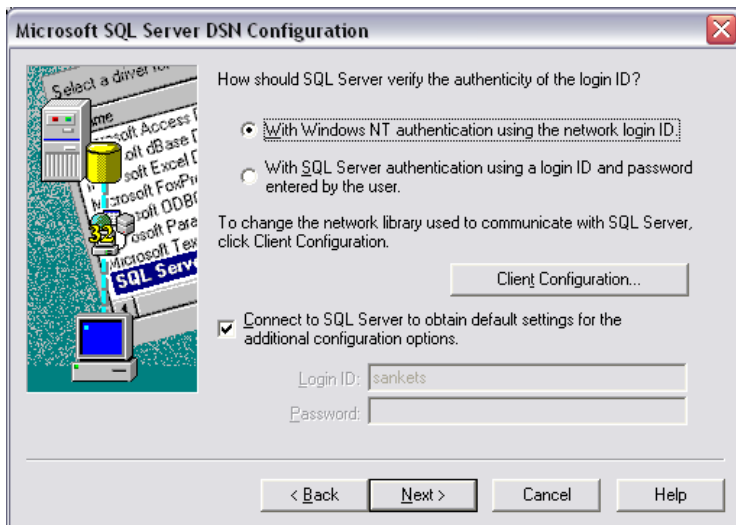


You should now see a list of drivers to choose from on the *Create a New Data Source* window.

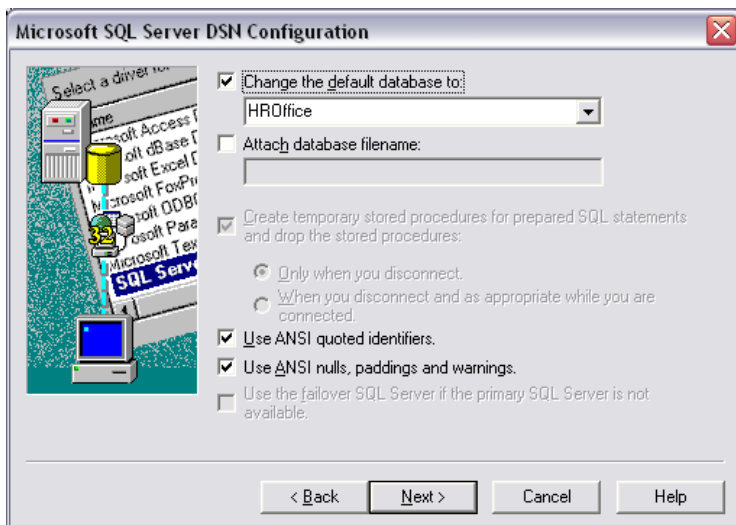
Select the *SQL Server* driver and click **Finish** to open the *Create a New Data Source to SQL Server* wizard which will guide you through the creation and testing of your new DSN.



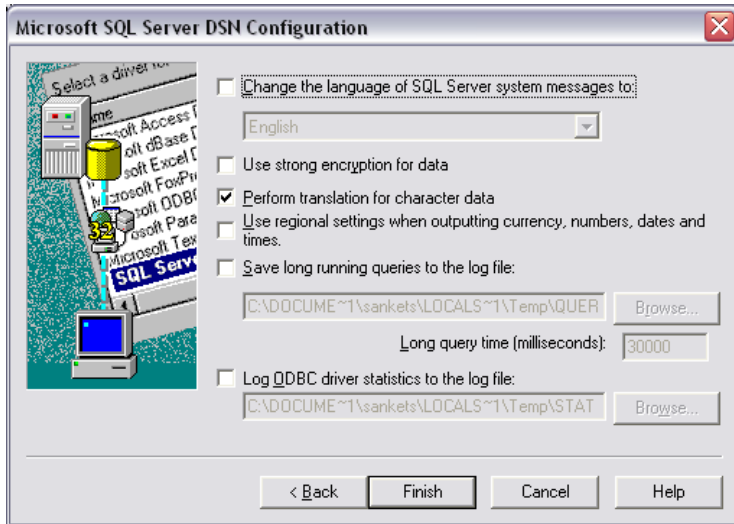
The first dialog in this wizard requires you to specify a name and description for the DSN you want to create, as well as the SQL Server you want to connect to. In the "Name:" field, type in "HROffice". In the "Description" field, type in "Ascentis HR Database". In the "Server" field, specify the SQL Server that houses your Ascentis HR database. Click **Next >** to continue



Next, select the authentication method you would like the DSN to use. The wizard will select "Windows NT Authentication, and check the "Connect to SQL Server to obtain default settings..." option by default. Click **Next >** to continue



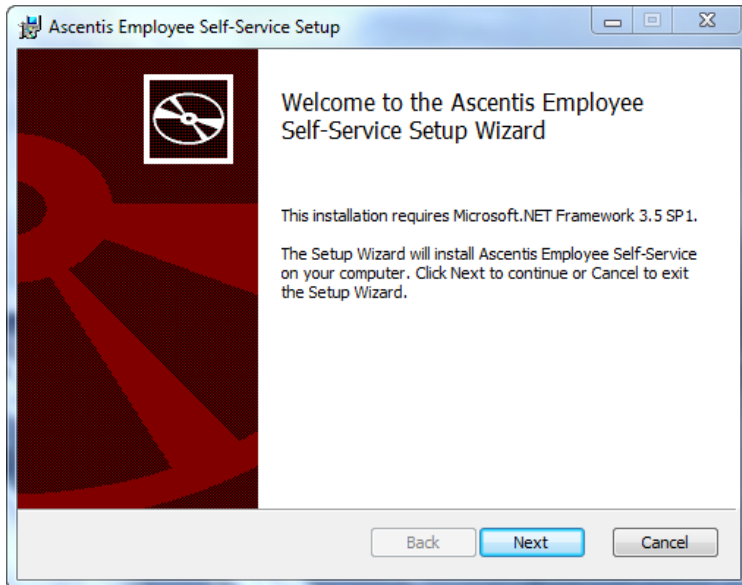
Check the "Change the default database to:" box and select the "HROffice" database from the list of available databases. The "Use ANSI quoted identifiers" and "Use ANSI nulls, paddings and warnings" boxes will be checked by default. Click **Next >** to continue to the final dialog in the wizard.



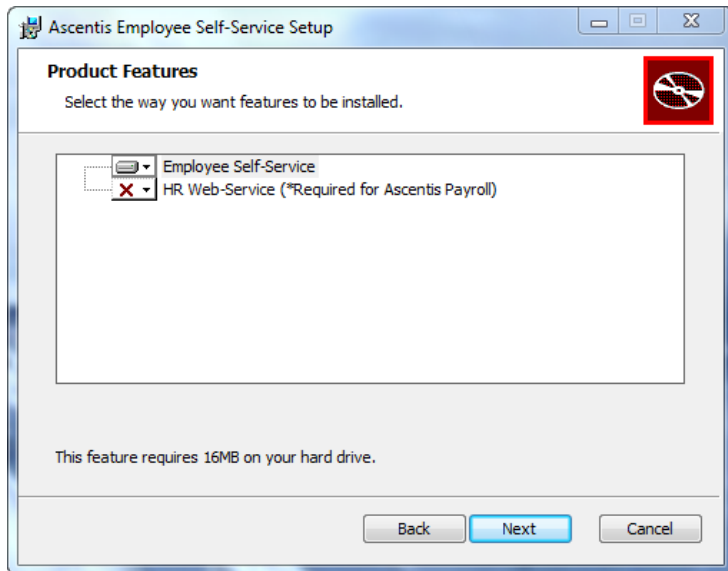
On the final dialog, simply accept the defaults and click **Finish** to complete the creation of your new data source. A new window will open up with a summary of your settings and the option to test that the data source can successfully connect to the Ascentis HR Database. Test now and make sure it passes.

STEP 3: Ascentis HR Self-Service Setup

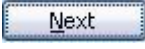
Once you have completed Steps 1 and 2, you are ready to install Self-Service.

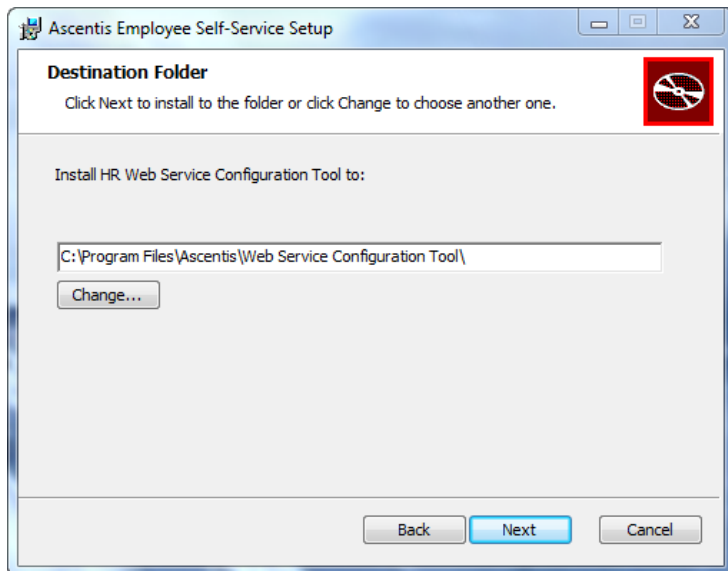


To continue installing Ascentis HR Self-Service, click **Next**

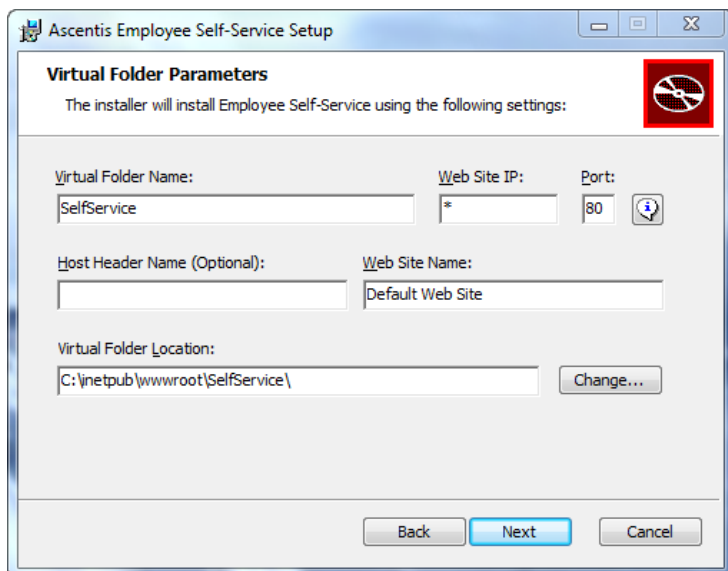


The "Employee Self-Service" feature is always enabled. The "HR Web-Service" is only required for Ascentis Payroll users and should not be installed by other users.

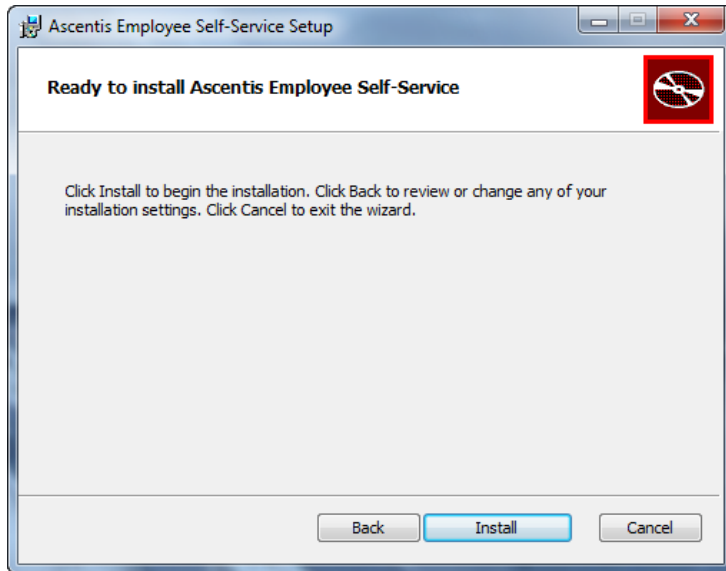
Click  to continue.



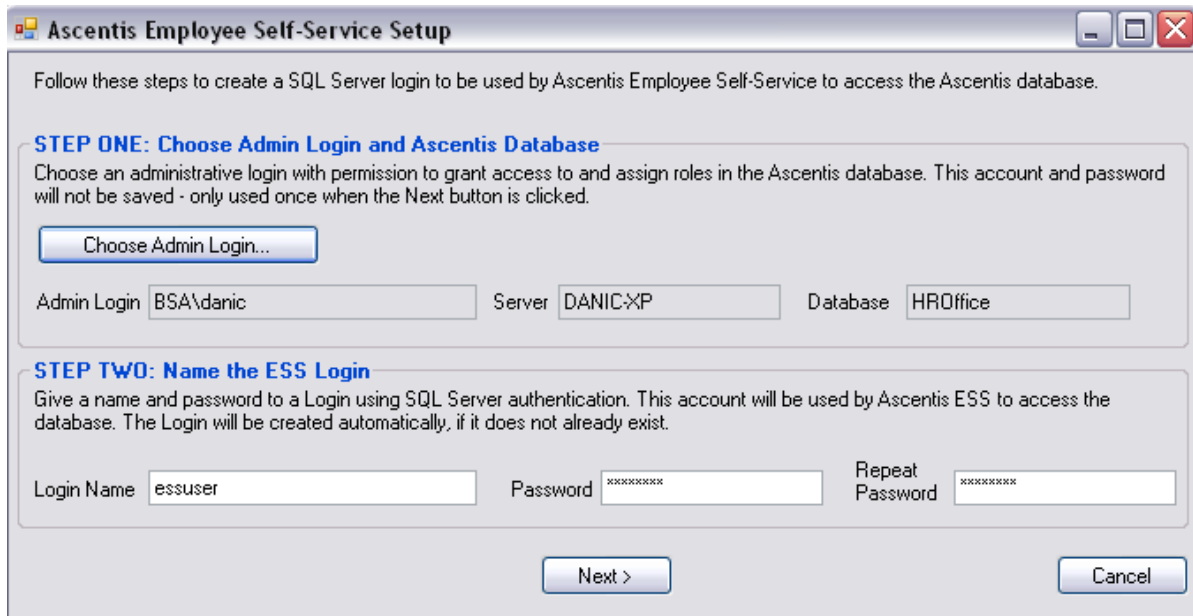
Type in the location of the of the Self-Service program files, this is where the HR Web Service Configuration Tool will install.



Enter the Virtual Folder parameters for Self-Service. Type in the Virtual Folder name, The Host Header Name is optional and can be left blank.



Click on the "Install" button. This will install and configure Self-Service.





Click on "Choose Admin Login..." and select the database server and database name of Ascentis HR (the logged in user must have credentials to access the SQL Server that Ascentis HR uses). Then create a SQL login name and password by filling in the fields. This account will be used by Ascentis Self-Service to access the database. Click and then to complete the install.

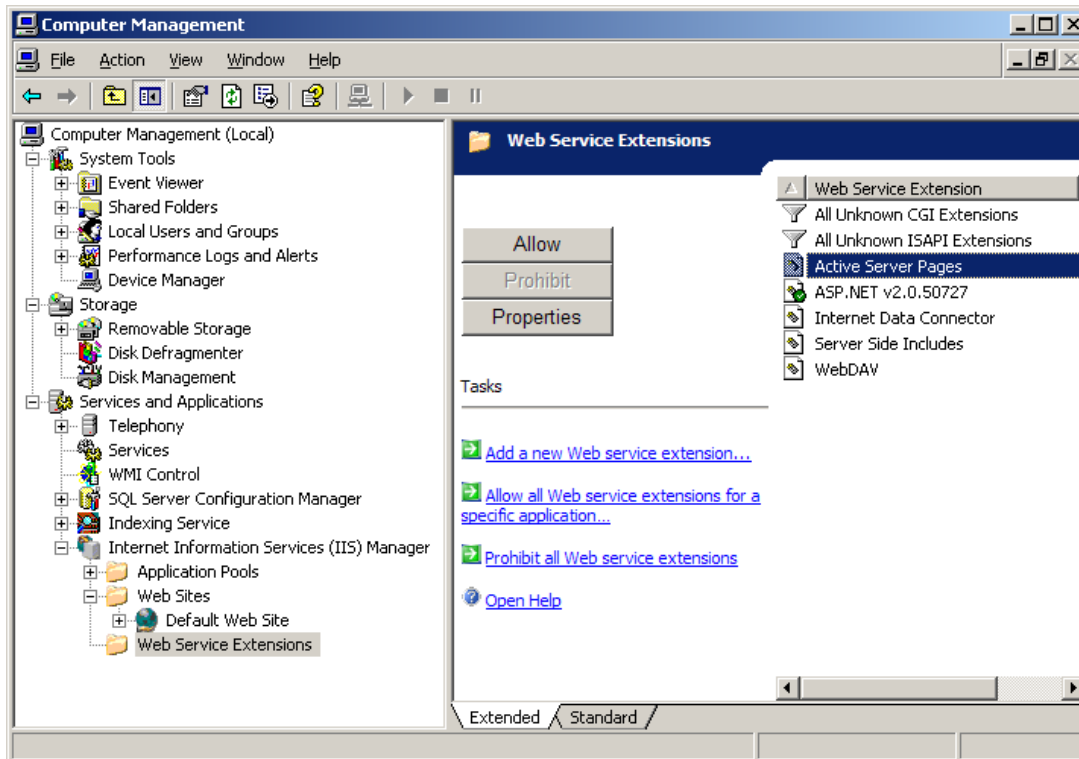
STEP 5: Additional Changes Needed for IIS

By Default, IIS 6.0 is locked down. It will be necessary to enable Active Server Pages and the .NET Framework in order to run Ascentis HR Self-Service.

From the *Control Panel* - open the *Administrative Tools* folder.



Double Click on the  Internet Information Services icon shown in the *Administrative Tools* folder. The *Internet Information Services* window will open. Double Click on the  **Web Service Extensions** icon and the right panel will show a list of Web Service Extensions.



Right click on Active Server Pages and click Allow.

Repeat the Process for ASP,NET V.2.0.x.

STEP 6: Setup SSL on the Web Server

If the intent is to run Self-Service over the internet, it will be necessary to setup Secure Sockets Layer (SSL) Encryption on the website that has Self-Service installed. To setup SSL you will need to obtain a SSL Certificate from a trusted provider and apply it on the Website.

By default, Self-Service will not run without SSL configured. If you plan to limit the deployment of Self-Service to your local area network, and do not wish to setup SSL, a manual configuration change will be required.

To allow Self-Service to work without SSL Encryption –

- Browse to the folder where Self-Service is installed. By default the folder name is Self-Service.
- From within this folder, find the *web.config* file and open in Notepad.
- Towards the bottom of the file, locate the *appSettings* section.

As detailed below:

```
<appSettings>
    <add key="RememberUserID" value="On"/>
    <!-- On or Off -->
    <add key="RequireSSL" value="Yes"/>
    <!--Yes or No -->
</appSettings>
```

Replace the "Yes" value to "No" – as detailed below:

```
<add key="RequireSSL" value="No"/>
```

Note: Applying this change and deploying Self-Service over the internet is not recommended.

EXTRA STEPS: Securing Your Web Server Machine

For added security these additional steps may be performed:

Clean up the web server machine by uninstalling all software that is not needed. For example, Windows Media Player has been the subject of recent hot fixes. Many programs are installed with Windows, by default, but are not needed on a web server.

Format the drives on the web server machine as NTFS drives. This allows you to grant the minimum access to directories needed by the IUSR account, protecting all other directories.

Install the web server and Self-Service on its own server machine, rather than combining it with domain controllers, file or database servers, etc. This helps you to simplify the environment the web server operates under, limit damage from a security breach, and improve performance.

Install IIS to a separate partition from the operating system (D: instead of C:). This will thwart directory traversal attacks, which look for files in "\\WINNT" or "\\WINNT\\SYSTEM32".