SpiraTeam® Administration Guide

Version 3.2

Inflectra Corporation

Date: December 18th, 2011

Contents

1. Introduction

SpiraTeam® is an integrated Application Lifecycle Management (ALM) system that manages your project's requirements, releases, test cases, issues and tasks in one unified environment:

SpiraTeam® contains all of the features provided by SpiraTest® - our highly acclaimed quality assurance system and SpiraPlan® - our agile-enabled project management solution. With integrated customizable dashboards of key project information, SpiraTeam® allows you to take control of your entire project lifecycle and synchronize the hitherto separate worlds of development and testing.

This administration guide outlines how to setup a working installation of either SpiraTeam®, SpiraTest® or SpiraPlan®, and how to perform routine administrative tasks.

It assumes a basic understanding of how to setup and administer a Windows 2003 Server®, Windows 2008 Server®, Windows XP® workstation or Windows Vista® workstation, and also assumes that you have access to a valid Administrator level account.

For information on how to use the features of SpiraTeam®, SpiraTest® or SpiraPlan®, please refer to the *SpiraTeam® User Manual* instead.

2. Installing SpiraTeam®

This section outlines how to prepare your system for installation of SpiraTeam®, how to actually install the software using the provided installation package, and finally how to ensure that your web-server is correctly configured to ensure secure operation.

The first sub-section will outline what hardware and software configurations are supported and the exact installation sequence for Windows 2008, 2003, 7, Vista and Windows XP. The second sub-section will explain how to load the SpiraTeam® software onto the server, and discuss common problems and solutions.

The minimum hardware and software requirements for running the SpiraTeam® system are:

Requirement	Minimum Specification
Processor:	Intel® or AMD® x86 or x64 compatible processor
Memory:	2 GB, 4 GB recommended
Operating System:	Windows Server 2008 (recommended) Windows Server 2003 (recommended) Windows 7 Windows Vista* Windows XP Professional*
Service Packs:	Windows Server 2003 SP2 Windows Vista SP1* Windows XP Professional SP2*
Database:	Microsoft SQL Server 2008 Microsoft SQL Server 2008 Express Edition Microsoft SQL Server 2005 Microsoft SQL Server 2005 Express Edition
Web Server:	Internet Information Services (IIS) 5.1 or higher ASP.NET Web Extensions 4.0 or higher
Web Browser:	Internet Explorer 7.0+ Mozilla Firefox 2.0+ Opera 9.0+ Google Chrome 0.4+ Apple Safari 3.0+
Other Components:	Microsoft Excel 2003+ (optional) Microsoft Word 2003+ (optional) Microsoft Project 2003+ (optional) Java Plug-In 1.6 (for screenshot capture applet)

*Note that SpiraTeam® can be loaded onto either Windows Server or Professional editions, provided that the IIS web-server is installed and that SQL Server is available as a database engine. However Windows Vista (except Ultimate edition) and Windows XP Professional can only support a maximum of 5 concurrent user web sessions. In general unless there are only going to be a couple of client machines hitting the server, we recommend using Windows Server 2003 or 2008.

2.1. System Prerequisites

Assuming that you have already installed the appropriate version of Microsoft Windows onto your computer (or that has been pre-installed for you), you need to then make sure that the various prerequisites have been correctly added to your installation before trying to install SpiraTeam®. The SpiraTeam® installer will check to ensure that the various prerequisites are in place, and will abort the installation if any are missing, indicating to you what action needs to be taken.

We recommend that you install / configure the prerequisites in the following order:

 ➤ Install SQL Server 2008 or 2005

 ➤ Install Internet Explorer 8.0 or 9.0

 ➤ Ensure that IIS is installed

 ➤ Install the .NET Framework v4.0

 ➤ Ensure that ASP.NET 4.0 is enabled

2.1.1. Install SQL Server 2008 or 2005

Install the appropriate version of the database software, following the instructions provided with the installation. We recommend SQL Server 2005/2008® Express Edition® for most users. This free version of SQL Server will offer sufficient performance for most installations and can be easily downloaded from either the customer area of our website or directly from the Microsoft® web-site at http://www.microsoft.com/express/sql.

2.1.2. Install Internet Explorer

Install the appropriate version of the browser (we recommend 8.0 or 9.0), following the instructions provided with the installation. You are free to use Internet Explorer, Mozilla Firefox, Apple Safari, Google Chrome or Opera with SpiraTeam®. Other browsers (Netscape, Konqueror, etc.) may work with SpiraTeam®, but they have not been exhaustively tested for compatibility by Inflectra®.

2.1.3. Ensure that IIS is installed

On Windows Server installations, IIS is usually installed as part of the factory configuration, whereas on Windows Vista and XP installations, you typically need to manually add the components to the factory configuration. The steps that you need to take to verify its installation are listed below for each operating system:

a) Windows XP or 2003 Server

To check if you have IIS installed, click Start > Control Panel > Administrative Tools. Under the "Administrative Tools folder", you should see an icon for "Internet Information Services". If you don't see this icon, then it means that you need to add IIS to your computer:
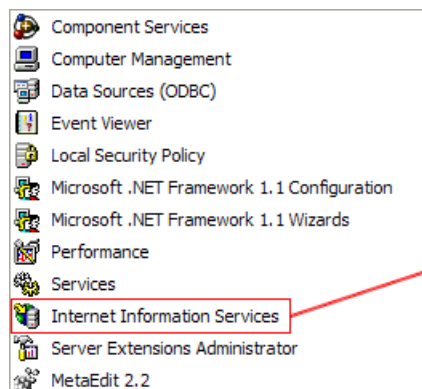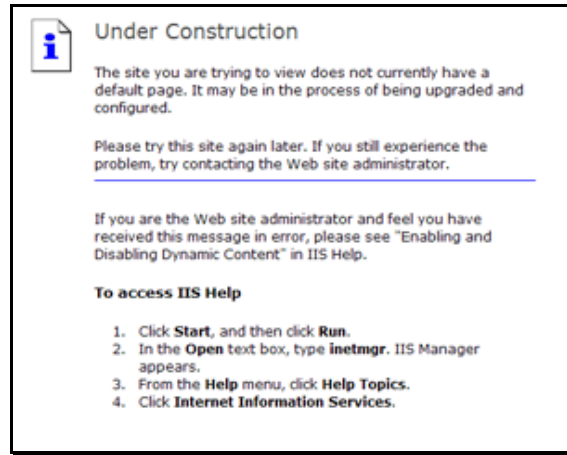
To install IIS, you need to click Start > Control Panel > Add or Remove Programs, then choose the option to "Add / Remove Windows Components" as illustrated below:
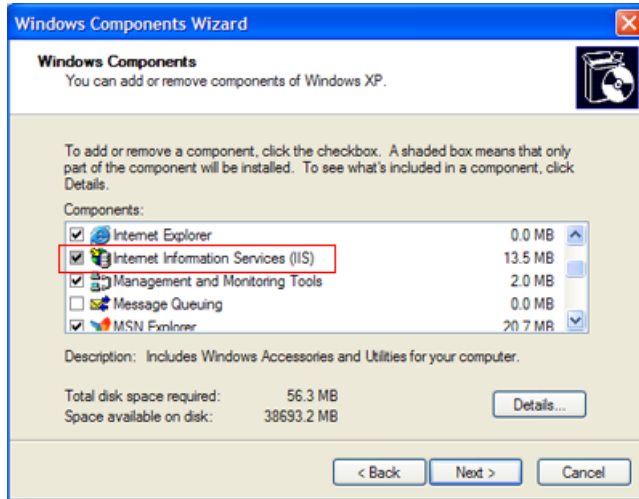
Check the box marked "Internet Information Services (IIS)", and click the <Next> button to install the missing Windows components. Once the installation has completed, IIS will now be installed on your system. To verify that this is the case, type http://localhost into the address bar of Internet Explorer on your computer. You should see a screen displaying the initial IIS startup page:

Windows XP IIS Default Page   Windows 2003 Server IIS Default Page

If you don't see this page, but instead see an IIS error page (e.g. Internal Server Error 500), please refer to *Appendix A – Troubleshooting IIS* to fix your IIS installation before following the rest of this installation guide.

On Windows 2003 Server you may also need to go into the Web Service Extensions folder and make sure that ASP.NET 4.0 is marked as 'Allowed'. If you receive an HTTP 404 (Page Not Found) error when running SpiraTeam® then it usually means that ASP.NET 4.0 is marked as Prohibited.

b) Windows Vista or 2008 Server

To check if you have IIS installed, click Start > Control Panel > Administrative Tools. Under the "Administrative Tools folder", you should see an icon for "Internet Information Services (IIS) Manager". If you don't see this icon, then it means that you need to add IIS to your computer:
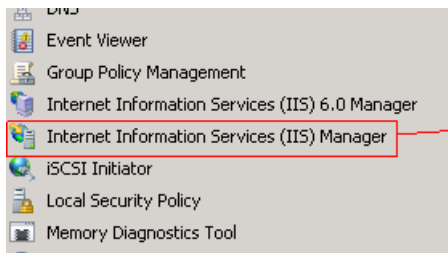
To install IIS, you need to click Start > Control Panel > Programs and Features, then choose the option to "Turn Windows features on or off". This will bring up the list of features and roles that can be configured on the server:
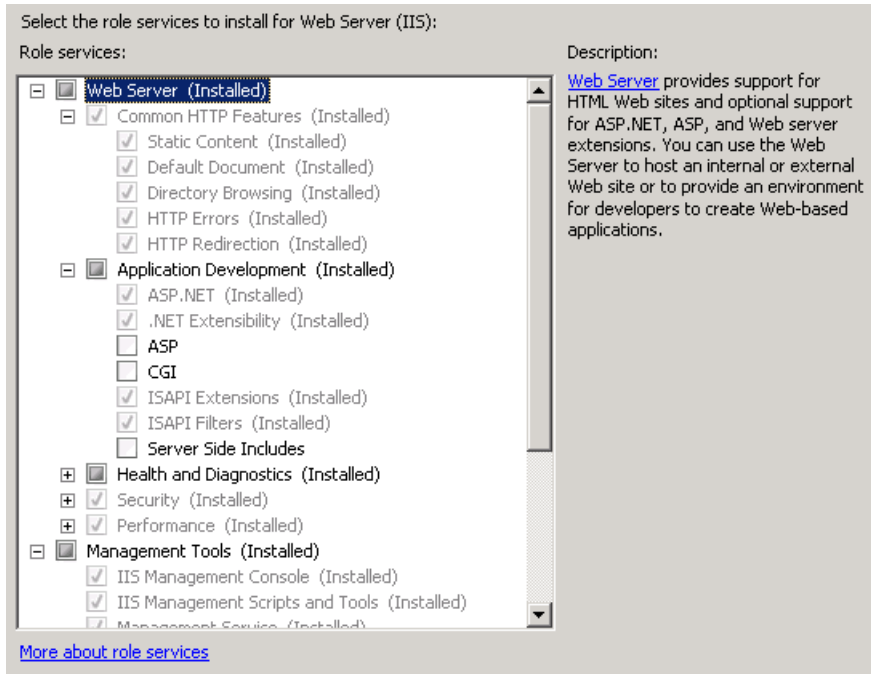
Make sure that the following features are enabled:

- ➤ Common HTTP Features
    - ▷ Static Content
    - ▷ Default Document
    - ▷ HTTP Errors
    - ▷ HTTP Redirection
- ➤ Application Development
    - ▷ ASP.NET
    - ▷ .NET Extensibility
    - ▷ ISAPI Extensions
    - ▷ ISAPI Filters
- ➤ Management Tools
    - ▷ IIS Management Console
    - ▷ IIS Management Service

To verify that this IIS is now installed, type http://localhost into the address bar of Internet Explorer on your computer. You should see a screen displaying the initial IIS startup page:

2.1.4. Install the .NET Framework v4.0

On Windows Vista, Windows 7 and Windows 2008 Server installations, Microsoft .NET Framework v4.0 is usually installed as part of the factory configuration, whereas on earlier operating systems, you might need to manually add the .NET 4.0 components to the factory configuration.

To see which version of the Microsoft .NET framework installed, open up Windows Explorer® and navigate to C:\WINDOWS\Microsoft.NET\Framework and then the subfolders listed will indicate which version(s) of the framework you have installed:
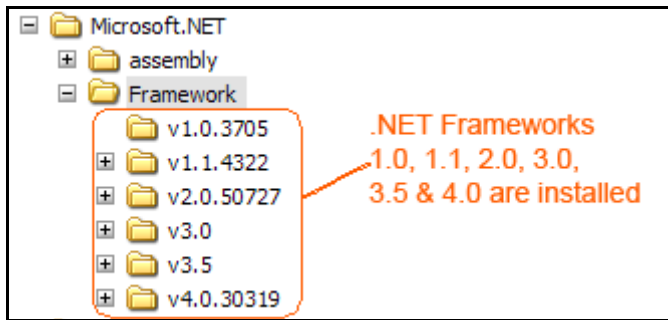
To install the .NET Framework, launch Internet Explorer and enter the URL: http://www.microsoft.com/netframework. From this page there will be links to download and install the latest version of the .NET Framework (version 4.0 at time of writing). Click on the option to download and install the .NET Framework, and follow the instructions provided. Once you have completed the install, verify that the installation was successful by looking in the "Administrative Tools" folder as illustrated above. You also need to make sure that .NET 4.0 has been installed if necessary.

Please make sure that the **Full .NET 4.0 Framework** is installed and not just the **.NET 4.0 Client Profile**. You can check which is installed by going to Start > Control Panel > Programs & Features and then looking for the different .NET 4.0 Framework components that are installed:
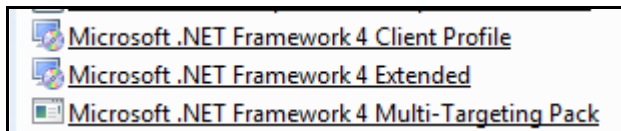

If you only see the "Microsoft .NET Framework 4 Client Profile" and not the "Microsoft .NET Framework 4 Extended", then you need to install the additional .NET 4.0 components that are needed for server-based applications such as SpiraTeam to run.

2.1.5. Ensure that ASP.NET is installed

Now that you have both IIS and .NET installed, you need to make sure that the Active Server Pages (ASP.NET) components that allow IIS to access the .NET framework have been correctly configured. If you installed .NET *after* IIS then ASP.NET is typically configured for you, but if you installed IIS afterwards, then further manual steps may be necessary. The settings are different depending on which version of Windows you are using:

a) Windows XP or 2003 Server

To verify that ASP.NET has been correctly configured, click on Start > Control Panel > Administrative Tools > Internet Information Services to launch the IIS administrative console:
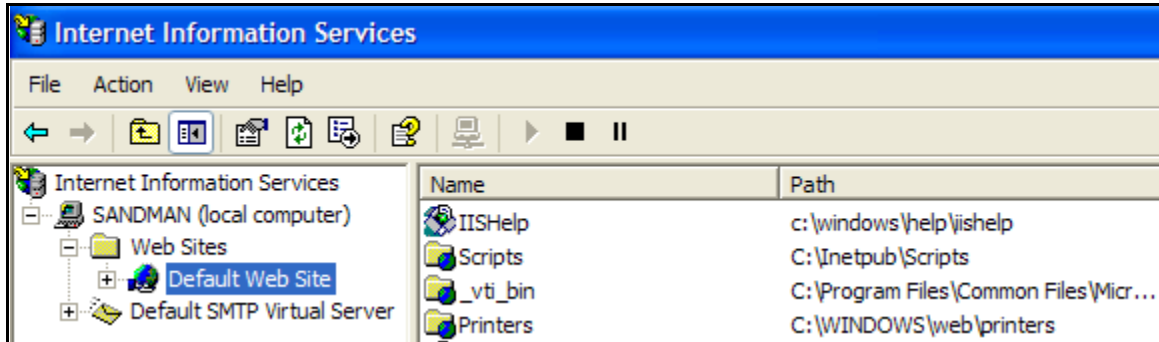
Expand the name of the web-server (marked as local computer), expand the "Web Sites" folder, right-click on "Default Web Site" and choose the "Properties" link. This will bring up the IIS configuration dialog-box with the 'Virtual Directory' tab highlighted. Then click on the 'ASP.NET' tab if it is listed:
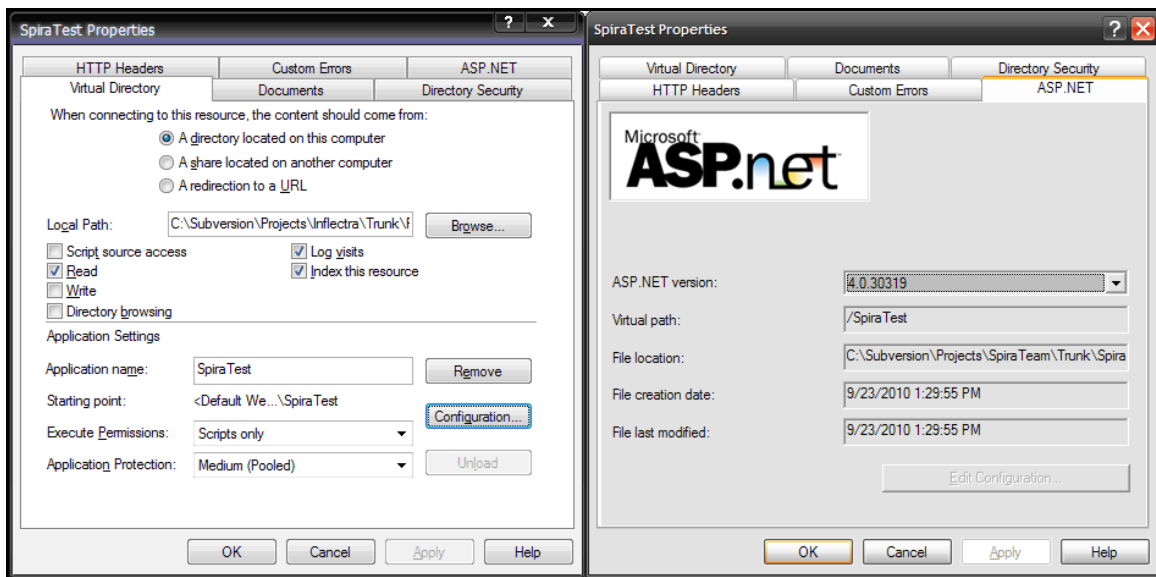
If ASP.NET 4.0 is correctly configured you will see the ASP.NET tab, and it will list the ASP.NET version as being '4.0.30319' as illustrated above. If you don't see this tab, you either don't have ASP.NET configured, or you have an earlier version of ASP.NET (v1.1 or v2.0) configured.

To configure ASP.NET 4.0 for an existing IIS website, you need to open up Windows Explorer and navigate to the folder containing the .NET Framework. So, for example, if you have .NET Framework v4.0 installed, you would navigate to C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319. Now, you need to open up a Windows command prompt by clicking Start > Programs > Accessories > Command Prompt. This will open up the command prompt window:
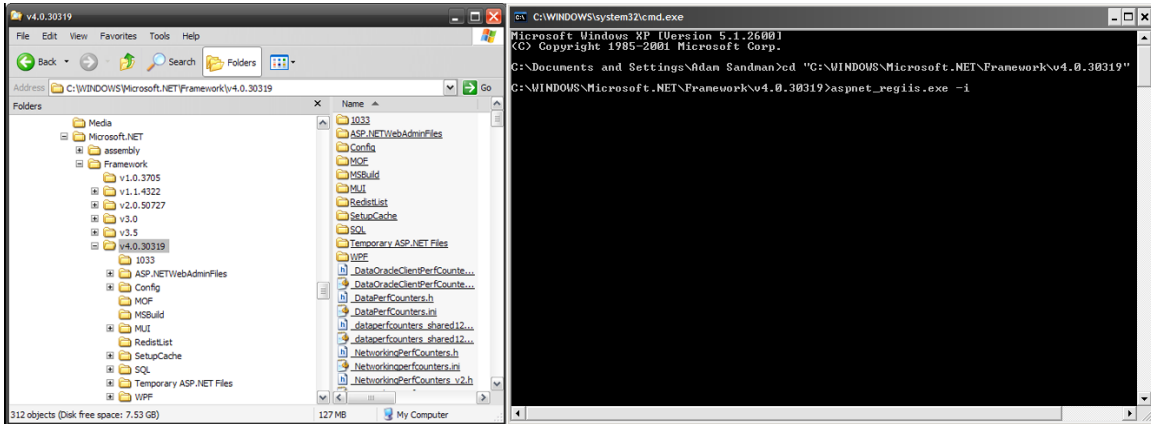
Now change the directory in the command window to the folder name in windows explorer (i.e. type <u>CD C:\ WINDOWS\ Microsoft.NET\ Framework\ v4.0.30319</u> where the version number matches the version number of the framework you have installed). Once you have changed the directory to the appropriate folder, simply type <u>aspnet_regiis.exe –i</u> to configure ASP.NET. You can now verify that ASP.NET has been installed by checking the IIS management console (as described above).

<u>b) Windows Vista, 7 or 2008 Server</u>

To verify that ASP.NET has been correctly configured, click on Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager to launch the IIS administrative console:
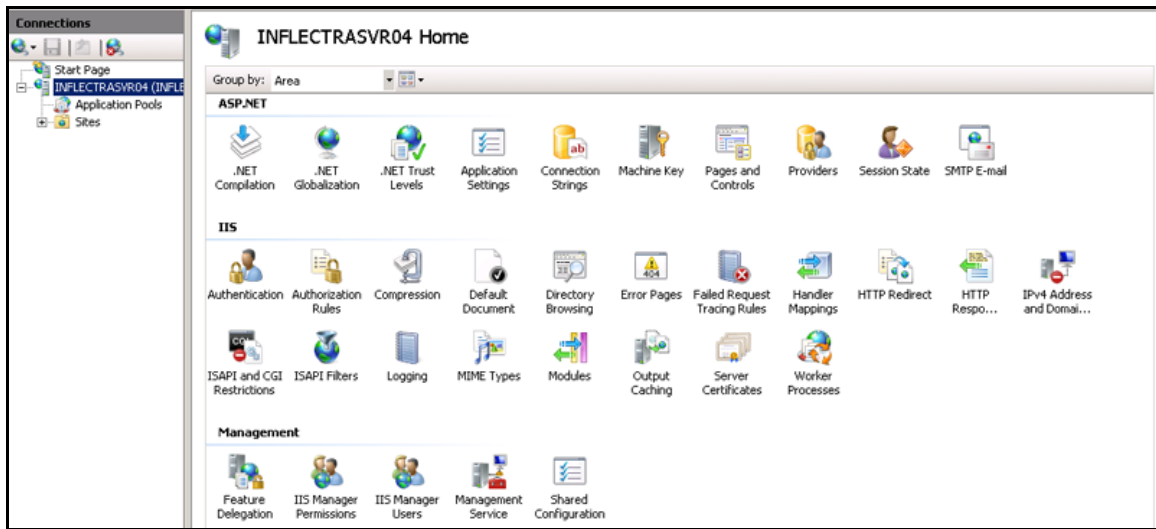
You should see a section called "ASP.NET" occupying the top third of the IIS screen. If not, then you need to go back to section 2.1.3 and make sure that you chose the option to install ASP.NET when installing IIS.

2.2. Installing the Software

Now that all the prerequisites have been correctly installed, you are now ready to install SpiraTeam® onto your system. To perform the installation, you will need the installation package downloaded from the Inflectra® website, the name of the organization that the software is licensed to, and the actual license key code which will be available in the customer area of the Inflectra® website.

To start the installation, double-click on the SpiraTeam® installation package (it will have a filename of the form `SpiraTeam-v3.x.x.x.msi`), and the Windows Installer will display the following dialog box:
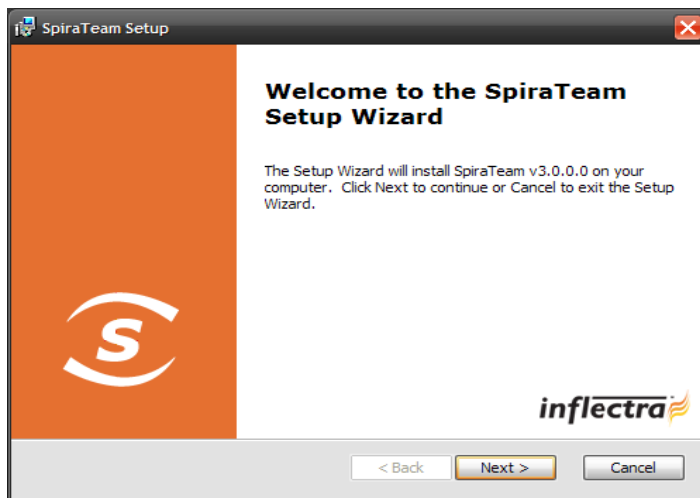
If you are upgrading from an earlier version of SpiraTeam®, the dialog box will be similar except that it will instead let you know that you are upgrading from an earlier version to the current one:
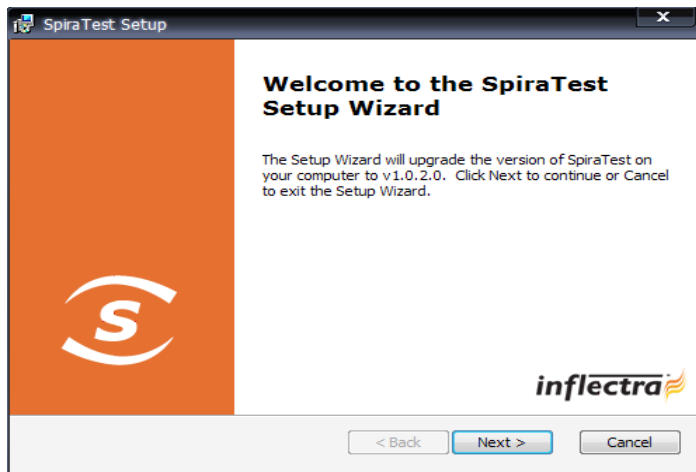
In this instance the installer will update the program files on your computer and migrate your data into the new version seamlessly. If for any reason you **don't see the upgrade message** and you have an existing installation, don't continue, but instead **contact Inflectra® customer support first**. This will ensure that your existing data is not overwritten by a clean install.

In either case, click the <Next> button to start the installation wizard which will gather information from you regarding how you want to setup the system, before actually installing the web-server files and database components. The next page of the installation wizard will display a list of all the required pre-requisites and whether the installer could find them or not:
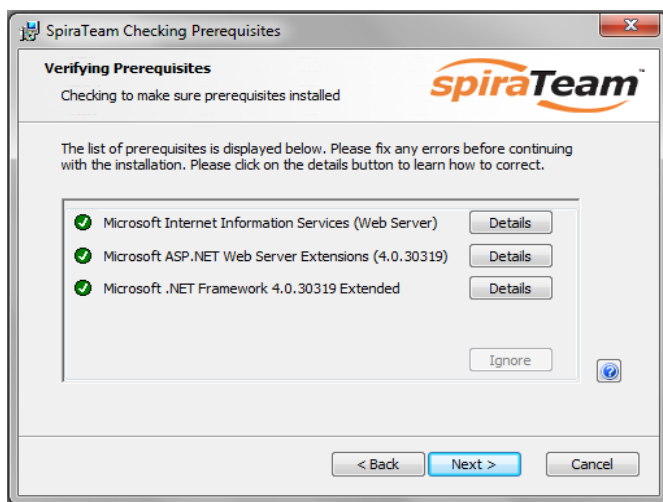
If any of the prerequisites were not correctly installed, the installer will display a red cross icon next to the missing component(s). If this happens, please refer to section 2.1 for installation of any prerequisites. If for any reason you have the prerequisite installed but the installer was not able to find it (this can occasionally happen on certain environments), click the <Ignore> button to proceed with the installation.

Once the prerequisites have been correctly installed, clicking <Next> will bring you to the next page in the installation wizard:

The next screen in the installation wizard outlines the SpiraTeam® End User License Agreement (EULA). Please read this carefully as it describes the legal contract between you – the user of the software – and Inflectra® Corporation, the developer and publisher. Once you have read the agreement and understood your rights and obligations, select the radio button marked "I accept the terms in the License Agreement" and click the <Next> button.

The following screen will be displayed:

You need to choose the product that you will be installing – SpiraTest®, SpiraPlan® or SpiraTeam®. This is important because the license key for each product is different.

Once you have chosen the product, the following screen will be displayed:
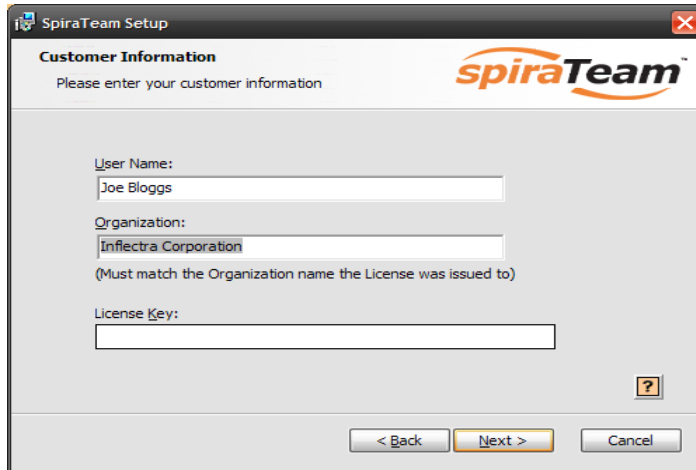
You need to enter your full name, the **organization that was issued the software license**, and finally the full hexadecimal license key that was provided with the software. Once you click <Next>, the installer will verify that all three were entered, and that the license key matches the product being installed and that it matches the organization name. The installer will warn you of any discrepancies, but will allow you to proceed; however after installation, the system will not operate until a correct license key is entered.

If for any reason you are unable to get the provided license key to work, please contact Inflectra[®] customer support immediately and they will resolve the issue.

After clicking <Next>, you will be given the choice of installation to perform:
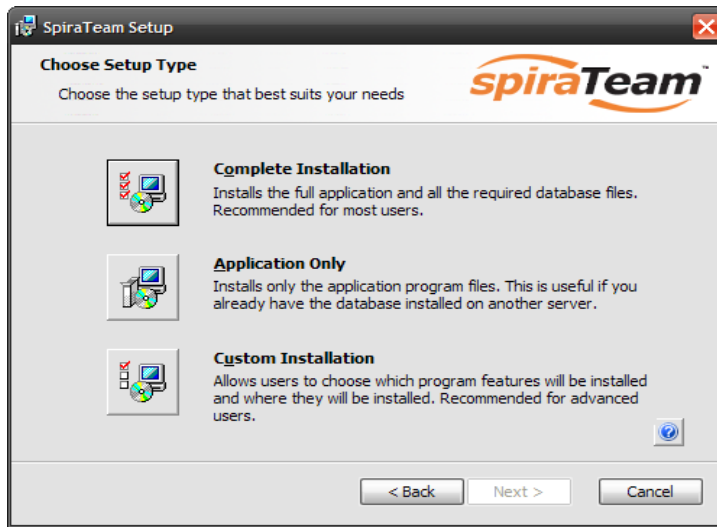
By default, the installer will install all of the SpiraTeam® features onto the target system, so we recommend choosing "Complete Installation", which will both install the complete system – application and database. For advanced users who want to change the folder to which the system is installed (by default it is `C:\Program Files\SpiraTeam`), change the name of the database created (by default it will be SpiraTeam) or to prevent the installation of the optional web-services data integration modules, you can choose the "Custom Installation" option, which allows you to change those settings prior to installation.

The "Application Only" installation is useful when you need to move the application to a different server, but want to leave the database installed on the same server. In this case you can use the "Application Only" installation on the new server, and once the installation is completed, change the name of the database pointed to in the "Web.Config" file to the existing database server.

This manual assumes that the "Complete Installation" option is chosen, in which case the following screen is displayed:
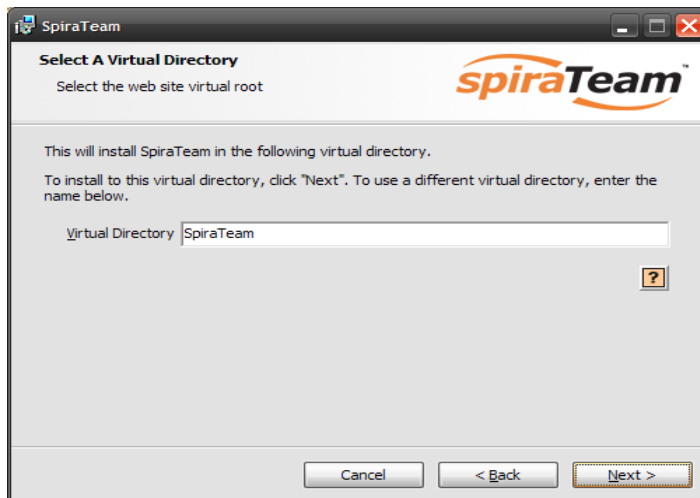
This screen allows you to change the name of the web-site URL that will be user to access the system. By default, users would need to type into their browsers: http://<server name>/SpiraTeam. Should you want to have a different name – other than SpiraTeam – change the name in the Virtual Directory box,

otherwise simply accept the default name and click <Next>. Note: The installer will check to make sure that the name you have chosen is not already in use, and will warn you if it is.

Upon clicking <Next>, you will be taken the database connection screen:
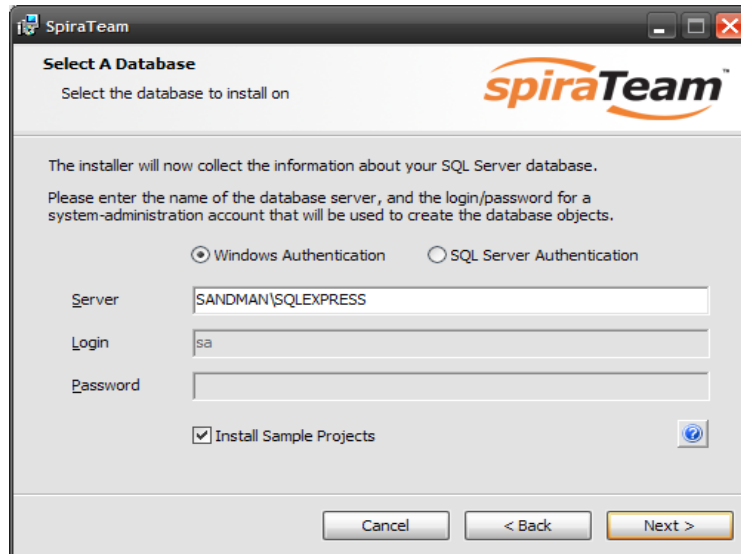
You can connect to the SQL Server database using either Windows Authentication or SQL Server Authentication, and the process is slightly different for each mode:

2.2.1. Windows Authentication

This is the easiest option when the application and database will be residing on the *same* server. In this case, choose the "Windows Authentication" option and the Login/Password boxes will be disabled. In this case, the installer will connect to the database using your current Windows login to create the application database objects, and SpiraTeam® will connect to the database during normal operation using either the ASPNET or NETWORK SERVICE Windows accounts (it depends on the version of the operating system).

2.2.2. SQL Server Authentication

This is the easiest option when the application and databases will be residing on *different* servers across the network. In this case, choose "SQL Server Authentication" and provide a SQL Server Login that has Database Owner (DB-Owner) permissions – e.g. the built in System Administrator (SA) account. The installer will use this DB-Owner account to create the database objects, and SpiraTeam® will use a special login (called SpiraTeam by default) for normal application operations.

For either mode, in the "Server" box, you need to enter the name of the Microsoft SQL Server instance that is running on your system; the installer will default it to the hostname of the server (which in many cases will be correct). The easiest way to find out the database server name is to open up the SQL Server Administrative console (typically by clicking Start > Programs > Microsoft SQL Server > Enterprise Manager) and look for the name of the server.

For SQL Server 2005/2008 Express edition installations, the Server name is usually the name of your computer followed by "\SQLEXPRESS", so for example, if your computer is called MyComputer, the server name would be MyComputer\SQLEXPRESS. Omitting the second part (called the instance name) would lead to a "host not found" error.

You can also choose whether to install the sample projects or not – typically we recommend installing the sample projects for evaluation installations and excluding them for production installs.

Once you have entered the various pieces of information, click <Next>. The installer will attempt to connect to the database using the provided information, and it will display an error message if any of the information is incorrect. Assuming the information is correct, the following screen will be displayed:
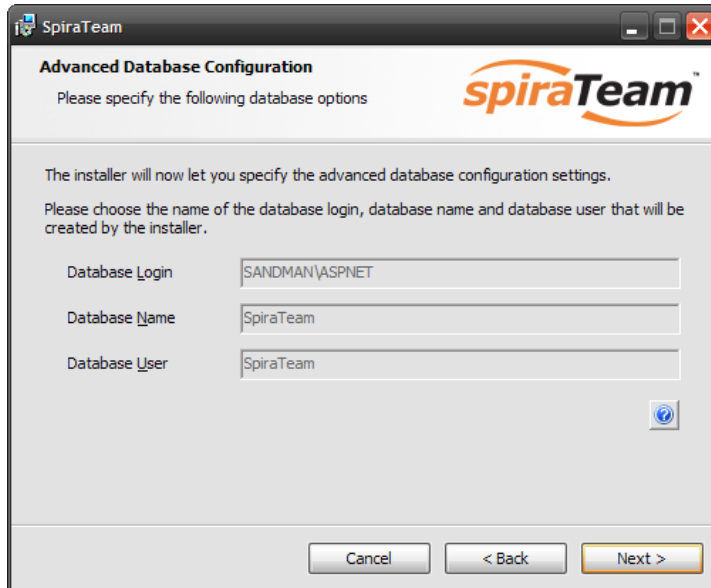

This page lets you customize the name of the database login, database name and database user that the application will create. If you chose the "Custom Installation", then the fields will be editable, otherwise they will be read-only. Also if you chose "Windows Authentication" then the Database Login field will be set to the built-in Windows account associated with ASP.NET for the specific operating system being installed on (and cannot be changed). Once you have reviewed this page and made any changes, you should click <Next> to proceed:
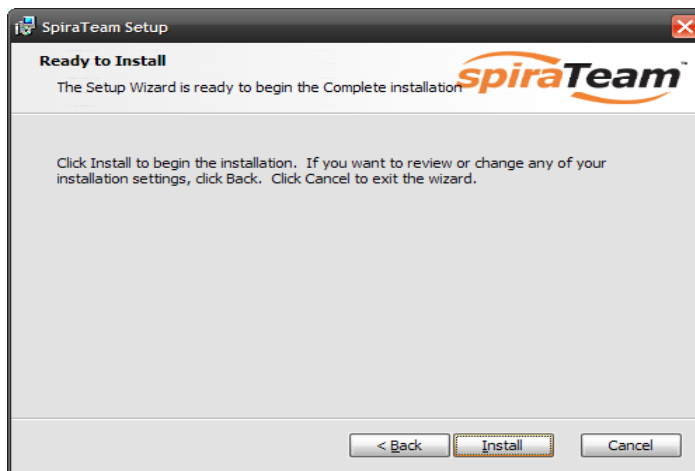
Click the <Install> button to actually begin the process of installing SpiraTeam® onto your system. If you are installing SpiraTeam® onto Windows Vista, then you will first be prompted by the Windows User Access Control (UAC) security system to confirm that you want to install a new piece of software. Click the option that confirms you want to proceed with the install.

The installer will then display a progress bar that gradually fills as the installation proceeds:
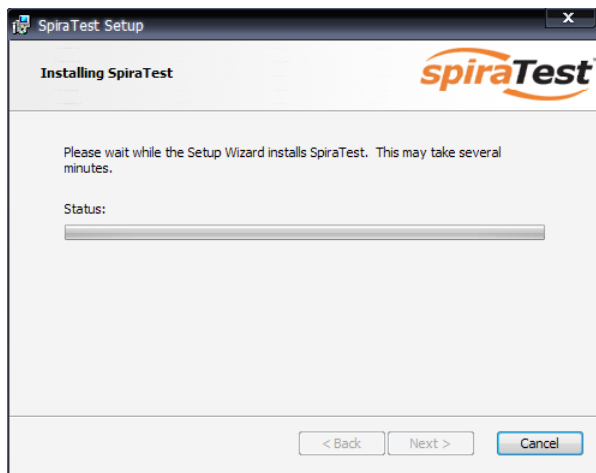
Once the installation is complete, the following message will be displayed:
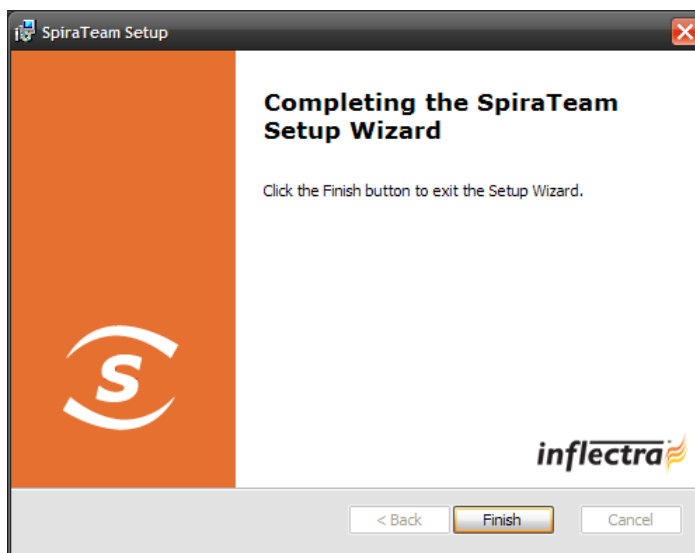
Congratulations! You have successfully installed SpiraTeam® onto your system. If you type http://localhost/SpiraTeam into your browser you should see the SpiraTeam® login page, as illustrated in the *SpiraTeam® User Manual*. If for any reason you don't see the login page, please refer to *Appendix A – Troubleshooting IIS* or contact Inflectra® Technical Support using one of the methods described at our website http://www.inflectra.com/Support.

2.3. Security Considerations

The Microsoft Internet Information Services (IIS) web-server and SQL Server database are powerful tools to managing web-based applications. However it is important to make sure that they are correctly secured to prevent unauthorized access to applications being hosted on them. This is a fast changing field and beyond the scope of this guide to address, however we recommend reading the following article for details on how to secure IIS:

 http://www.windowsecurity.com/articles/Installing_Securing_IIS_Servers_Part1.html

In addition to the steps outlined in this article, it is important to note that by default, all web pages served by IIS using the HTTP protocol are unencrypted, and as such, the usernames and passwords used by SpiraTeam® to log into the application can be read by network sniffing tools. If you are using SpiraTeam® purely within an intranet environment, this may not be an issue. However if you are externally hosting

SpiraTeam® onto a publicly accessible website, we recommend installing a Secure Sockets Layer (SSL) encryption certificate, and restricting all web-traffic to the secure HTTPS protocol instead. For details on how to perform this task, please refer to *Appendix B - Installing an SSL Certificate*.

3. System Administration

Now that you have successfully installed SpiraTeam®, this section of the guide outlines how to perform the typical system-wide administrative tasks necessary for setting up projects in the system, managing users and verifying the license information. To perform these tasks, you need to login to the system with a username that has "System Administration" permissions. The special "Administrator" username is created by the installer for this very purpose. You should initially login to SpiraTeam® with the username `Administrator`, and the password `PleaseChange`. It is recommend that this password be changed as soon as possible to something that is secure yet memorable by clicking on the "User Profile" link – see the SpiraTeam® User Manual for more details.

Once you have logged in as the Administrator, you need to click the "Administration" link above the main navigation bar. This will display the Administration home page:
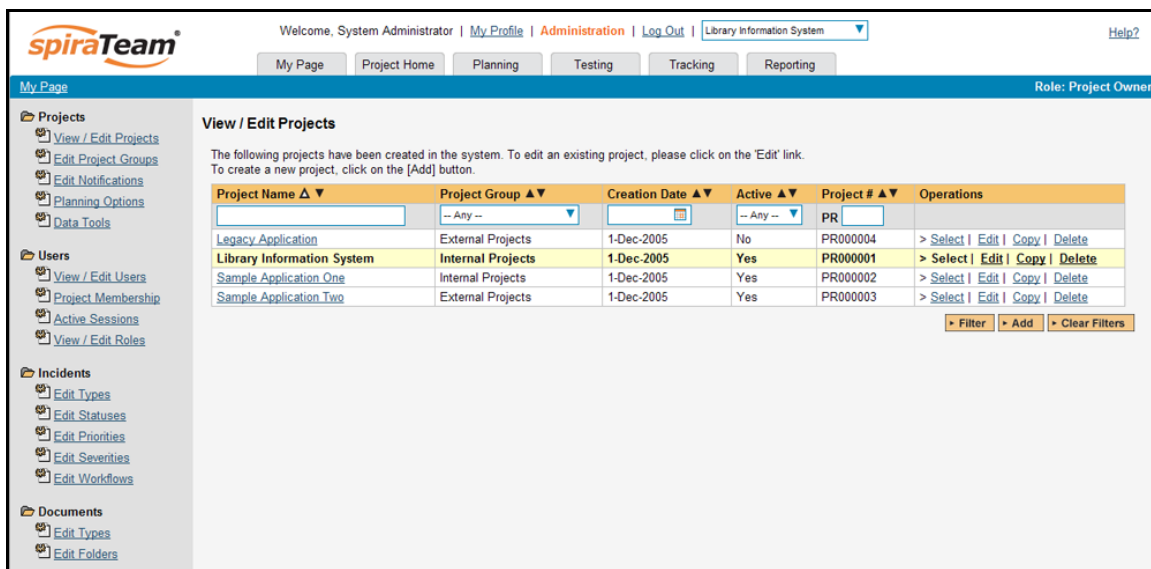
The Administration home page is divided into two main areas – the left hand navigation bar that contains links to all the available administration options (grouped under folders) and the main pane that displays the available settings for the selected option. By default, the "View/Edit Projects" administration screen will be displayed in the main pane.

The options available to you in the left hand navigation bar will vary depending on your level of administrative privileges. If you have the "system administration" privilege granted, then all the options will be available, whereas if you are just a "project owner", only those options relating to managing a specific project will be available.

When you first install the system, the three main tasks you will need to perform as the system administrator are creating/editing projects, creating/editing users and then adding the users as members of the various projects. These tasks typically need to be performed before any other users can use the system, since there will be no logins or projects available other than the sample ones provided during the installation.

Each of the individual administrative options is described in turn below:

3.1. Projects

3.1.1. View/Edit Projects

The following screen is displayed when you choose the "View/Edit Projects" link from the Administration sidebar navigation:

This screen displays the list of projects in the system (both inactive and active) together with their project group, date of creation and active status. Clicking on either the "Select" link in the right-hand column or the name of the project will change the currently selected project to one clicked, and any project-specific administration tasks will be applied to this project.

You can filter the list of projects by either choosing an active status, project group, or entering a portion of the name or date into the appropriate text box. When you click the <Filter> button, the list of projects will be filtered by the criteria you entered. You can clear the filter selection by clicking the <Clear Filters> button. To sort the list of projects, just click on the appropriate arrow icon located in the header row of each field (one each for ascending / descending) In addition, the list of projects is paginated into groups of fifteen (15). You can step through the different pages by clicking the page numbers at the bottom of the project list.

To permanently delete a project, you should click the "Delete" link to the right of the project details. This is irreversible and will delete all the artifacts associated with the project. If you want to temporarily delete a project, simply set its Active flag to 'No' instead. To make a copy of a project to reuse its test cases, releases, test sets and requirements, simply click the "Copy" link to the right of the project. *Note that this will not make a copy of any historical information, test runs or incidents.*

To add a new project to the system, simply click the <Add> button at the bottom of the project list, and a new screen will be displayed that allows you to enter the new project information:

You need to enter a name for the project (which cannot be the same as any already in use); select which project group it belongs to and optionally enter a detailed description and/or web-site URL. You should initially make sure that the project is marked as "Active". In addition, you can choose to either use the "default template" or to use an existing project as the template. Using an existing project as the template will copy across the workflows, user membership, custom properties, document types, document folders, data synchronization and other configuration settings that you want to reuse in the new project. Once you are satisfied with the information, click the <Insert> button to actually create the new project.

In a similar way, to edit the details of an existing project, simply click the "Edit" hyperlink in the right hand column of the project list box, and you will be taken to the following screen that allows you modify the project details:

On this screen you can edit the name, description, project group, website URL and active status. Once you have made the necessary changes, click the <Update> button to commit them. If you decide that you want to ignore the changes, click the <Cancel> button and the changes will be discarded.

3.1.2. Edit Project Groups

The following screen is displayed when you choose the "Edit Project Groups" link from the Administration sidebar navigation:

This screen displays the list of project groups in the system (both inactive and active) together with their web site URL, date of creation and active status. Project Groups are used to relate projects that are in the same department/division/organization or are for a common customer, client, etc. When projects are in the same group, a user that is a member of the project group can see the special Project Group Dashboard that displays key metrics from all the projects in the group combined. Also such users will have observer-level access to the contained projects without needing to be explicitly added to each project.

You can filter the list of project groups by either choosing an active status, or entering a portion of the name, web-site or date into the appropriate text box. When you click the <Filter> button, the list of project groups will be filtered by the criteria you entered. You can clear the filter selection by clicking the <Clear Filters> button. To sort the list of project groups, just click on the appropriate arrow icon located in the header row of each field (one each for ascending / descending) In addition, the list of project groups is paginated into groups of fifteen (15). You can step through the different pages by clicking the page numbers at the bottom of the project list.

To permanently delete a project group, you should click the "Delete" link to the right of the project group details. Any projects contained in the group will <u>not</u> be deleted, but instead just moved to the default project group. There has to be at least one project group in the system at all times, so the project group designated as the 'default' one will not be available for deletion.

To add a new project group to the system, simply click the <Add> button at the bottom of the project group list, and a new screen will be displayed that allows you to enter the new project group information:

You need to enter a name for the project group and optionally enter a detailed description and/or web-site URL. You should initially make sure that the project group is marked as "Active". In addition, you can choose to make this project group the default one (meaning that it cannot be deleted and projects get added to it when their groups are deleted). Once you are satisfied with the information, click the <Insert> button to actually create the new project group.

In a similar way, to edit the details of an existing project group, simply click the "Edit" hyperlink in the right hand column of the project group list box, and you will be taken to the following screen that allows you modify the project group details:

On the top part of this screen you can edit the name, description, website URL, active status and default status. Once you have made the necessary changes, click the <Update> button to commit them. If you decide that you want to ignore the changes, click the <Cancel> button and the changes will be discarded.

In addition, the lower part of the screen allows you to view/edit the users that are members of the group and also see which projects are in the group:

a) Group User Membership

This tab allows you to see which users are members of the group and which group role they have:

✓	Full Name	User Name	Project Group Role
☐	Fred Bloggs	fredbloggs	Group Owner ▼
☐	System Administrator	administrator	Group Owner ▼

▸ Update ▸ Add ▸ Delete

The two project group roles are "Executive" and "Group Owner":

➤ **Executive** – This role allows the user to see the dashboard for this project group, which contains all the key metrics for the contained projects displayed in an aggregated manner. Please see the *SpiraTeam User Manual* for more details on this dashboard. In addition, the user is automatically granted 'observer' permissions for all the projects in the group.

➤ **Group Owner** – This role consists of all the permissions granted to the "Executive" role above, but in additional allows the user to make changes to the Project Group itself in the Administration section.

To change the role of an existing project group member, just change the role in the drop-down list and click [Update]. To remove a member from the group, just select the appropriate checkboxes and click [Delete]. Finally, to add a new user to the group, click on the [Add] button:

Add Project Group Membership | Internal Projects

<< Back To Project Group Membership

The following users are NOT members of this project group.
Please select a role for the users you want to add to the project group and click [Add]:

First Name △▼	MI △▼	Last Name △▼	User Name △▼	User # △▼	Project Role
				US	
Joe	P	Smith	joesmith	US000003	--- Select Role --- ▼

▸ Filter ▸ Clear Filters ▸ Add ▸ Cancel

You now should narrow down the list of users by entering filter criteria and clicking [Filter]. Once you have located the appropriate user(s), just select a group role for them from the drop-down list and click [Add] to add them to the group in the specified role.

b) Group Project List

This tab allows you to see the list of projects that are contained within the current group. Clicking on the name of the project will take you to the details page for that project:

User Membership	Project List			
Project Name	**Web Site**	**Creation Date**	**Active**	**Project #**
Library Information System	http://www.libraryinformationsystem.org	1-Dec-2005	Yes	PR000001
Sample Application One	http://www.tempuri.org	1-Dec-2005	Yes	PR000002

3.1.3. Planning Options

This screen is available for installations of SpiraPlan® and SpiraTeam® only (not SpiraTest®) and allows you to configure the schedule and calendar options for the various project estimation and planning modules. The settings are specific to each project:

This page allows you to make changes to the following settings:

➤ **Work Hours Per Day** – this setting allow you to specify how many work hours should be used when converting an effort calculation from hours to calendar days. For example a 12 hour task will occupy two days if you set the working hours per day to 6 hours, whereas the same task will occupy 1 ½ days only if you set the working hours per day to 8 hours.

➤ **Work Days Per Week** – this setting allows you to specify how many days in the week are *typically* worked on the project. By default the system assumes a 5-day (Mon-Fri) working week, but if your organization works Saturdays (for example), you may want to switch to a 6-day working week. If you want to use partial days, then just round up to the nearest day and add non-working hours (see below) to compensate.

➤ **Non-Working Hours Per Month** – this setting allows to specify how many non-working hours *typically* need to be accounted for. This is useful if you want to have a working week that contains a fractional number of days or if you have recurring activities that need to be removed from each month. *Note that if you have specific holidays, vacation days that need to be accounted for, it is better to use the Release/Iteration non-working time feature instead.*

➤ **Effort Calculations** – When calculating how much effort has been scheduled in a release or iteration, the system will aggregate the individual effort values (both estimated and actual) for all the task and incident artifacts associated with the release/iteration. This setting allows you to specify if you want only task or incident effort values to be included in the release/iteration total. This is useful if your project management methodology requires that incident effort values be excluded from the total.

➤ **Time Tracking** – SpiraTeam® has an integrated time tracking system that allows the easy entry of the hours spent on all assigned incidents and tasks in one place (see the *SpiraTeam User Manual* for more details on this feature). This setting allows administrators to specify if they want the integrated time tracking features enabled for both incidents or tasks (or neither).

➤ **Default Effort** – Normally when you create a new Requirement or Task in the system it will be given an empty initial estimated effort. However if many requirements or tasks are typically based on a standard size, then as a time-saver, the system will let you specify a default estimated effort that will be used when a new requirement or task is created.

➤ **Auto-Create Tasks** – When you change the status of a Requirement in the system to "In-Progress" the system will automatically add a default Task to that requirement if no tasks already exist. This is a useful shortcut that makes planning with requirements easier in the case when the requirements are of a size where they don't need to be formally decomposed into multiple developer tasks. However if you don't want the system to automatically create tasks in, you can deselect the option for the current project and it will turn off the feature.

3.1.4. Project History

This page displays a list, by default in chronological order, of changes made to items within the selected project.

At this time, only changes made to Requirements, Tasks, Incidents, Test Cases, Test Steps, Test Sets, Releases, and Automation Hosts are recorded. Certain changes are to these artifacts are not recorded, such as location changes (indenting, outdenting), and comment additions.

✓	Change ID ▲▼	Change Date ▲▽	Changed By ▲▼	Artifact Type ▲▼	Artifact ID ▲▼	Change Type ▲▼
☐		🗓	-- Any -- ▼	-- Any -- ▼		-- Any -- ▼
☐	#15	27-May-2011	System Administrator	Incident	3	Deleted
☐	#14	27-May-2011	System Administrator	Incident	3	Modified
☐	#13	2-May-2006	Fred Bloggs	Incident	7	Modified
☐	#12	2-May-2006	Fred Bloggs	Requirement	4	Modified
☐	#11	2-May-2006	Fred Bloggs	Test Step	3	Modified
☐	#10	2-May-2006	Fred Bloggs	Release	1	Modified
☐	#9	2-May-2006	Fred Bloggs	Test Case	2	Modified
☐	#8	5-Mar-2005	Fred Bloggs	Incident	7	Modified
☐	#7	5-Mar-2005	Fred Bloggs	Incident	6	Modified
☐	#6	4-Mar-2005	Joe P Smith	Incident	7	Modified
☐	#5	4-Mar-2005	Fred Bloggs	Incident	6	Modified
☐	#4	4-Mar-2005	Joe P Smith	Requirement	4	Modified
☐	#3	4-Mar-2005	Joe P Smith	Test Step	3	Modified
☐	#2	4-Mar-2005	Joe P Smith	Test Case	2	Modified
☐	#1	4-Mar-2005	Joe P Smith	Release	1	Modified

Displaying 1 - 15 out of 15 items. Refresh | Apply Filter | Clear Filter

Show 15 ▼ rows per page ◄◄ ◄ Displaying page 1 of 1 ►►

▶ Revert ▶ Purge All

There are a handful of change types recorded and displayed here:

• **Modified**: The most common, this means that one or more fields in this artifact were changed. Note that if a standard field and a custom field were changed at the same time, it will generate two separate entries, one for the standard fields, one for the custom fields.

• **Added**: This means that this artifact was added, created in the system, either by using the New menu option or by copying. Pasting an item that was cut will not result in an Added entry being created.

• **Rollback**: This items means that the artifact was rolled back to a specific event in the history.

• **Deleted**: This entry is created when an artifact is deleted from the system.

- **Undelete**: This entry is created when an artifact was deleted and then undeleted, making it live in the system again.

- **Purged**: This entry is created (and all other history items are removed) when a deleted artifact is purged from the system. Purged items are removed from the database, and cannot be recovered.

Note: When upgrading from a version before v3.1, each individual field changed will be considered a unique change, due to how previous versions recorded history. However, as soon as the application is upgraded, simultaneous changes will be grouped together based on their last-update date.

This screen allows the administrator several options:

- *Viewing Details*: The detail screen for each change set can be viewed by clicking on the change ID #. This will take you to the history details screen, described below.

- *Revert*: This button will roll back all items in the list that are checked. You must have at least one row checked to revert. See the section on reverting below.

- *Purge All*: This button will permanently purge all deleted items from the database. Once items are purged, they cannot be restored.

3.1.4.1 History Details Screen

The history details screen displays information on the selected change set:

History Details | Library Information System (Change Project)

The details for this changeset are listed below.

This artifact has been deleted.

Change: **14**   Change Date: **5/27/2011 10:36:30 AM**
User: **System Administrator**   Change Type: **Modified**
Artifact: Incident [IN:3]   Field Set: **Standard Fields**

Change Actions

Field Name ▲▼	Old Value ▲▼	New Value ▲▼
Priority		2 - High
Severity		3 - Medium
Type	Incident	Enhancement
Detected By	Fred Bloggs	System Administrator
Detected Release	1.0.1.0	1.0.1.0.0001

The History Details screen will show basic information as well as fields that were changed in this change set. Shown here is the Change ID, the date and time that the change was made, the user that made the change, the change type, the artifact affected, and the set of fields affected.

If a set of fields were affected (Standard or Custom), then the list of fields will be listed below. In the example above, the change was a Modification, and 5 fields were changed. In other change types, no fields will be displayed.

If the artifact is still available in the system, you can click the Artifact or click the 'View Item' button in the toolbar to view the item as it is currently. However, if the item has been deleted, a warning label will be displayed (as above in the example screenshot), the View Item links will be disabled, and a new option, "Purge" will appear on the toolbar.

3.1.4.2 Purging Items

Items that have been deleted by any user still remain in the database, but do not affect statistics or reports, and do not show up in reports and cannot be viewed. The artifacts are still in the database, however, and can be restored by clicking on the Restore button in the toolbar.

Purging an individual item can only be done while viewing one of its history detail screens. Once an item is purged, you will be taken back to the history list screen. All the previous history items for the artifact will be removed, and replaced with a single "Purged" history item.

Items that are purged cannot be restored into the database, as unique identifiers will be wiped from the database, so be sure that you are sure you want to purge an item before doing so.

You can purge all items in the project at once by clicking the "Purge All" button located on the History List page. This will take some time depending on how many deleted items are in your database, and it is recommended that the database files be compressed in SQL Management Studio afterwards to free up space and compress clustered indexes.

3.1.4.3 Reverting Items

Reverting an artifact will attempt to reset all fields back to the selected change set, reverting all changes made after the selected change set as well. In certain cases, the artifact will not be able to be reverted – cases like this could be caused by other items having been deleted or purged. (For example, if Requirement #1 was linked to Release #4, and that Release does not exist anymore.) In cases like this, no fields will be reverted and the artifact will remain unchanged.

Reverting an item will cause it to be undeleted if it has been deleted.

You can revert multiple items from the History List page – however, the only items that can be reverted back are Deletes and Modifications. All other types will be ignored. When selecting multiple items, you can select more than a single change set for a specific artifact, the artifact will be rolled back to the earliest change set selected.

3.1.5. Project Data Tools

This page contains several different data management tools that can be used to identify certain data issues in the system and correct them. There are two main sections to this page – Data Caching and Indentation Hierarchy:

Project Data Tools | Library Information System *(Change Project)*

In order to improve the performance of the application, SpiraTeam caches certain types of data. Sometimes after making changes to the underlying data, you might want to refresh the cached information. To do that, click on one of the links below:

> Refresh the Test Status Information
> Refresh the Task Progress Information
> Correct Requirement Indents (Current status: OK)
> Correct Test Case Indents (Current status: OK)

<u>a) Data Caching</u>

In order to improve the performance of SpiraTeam®, certain types of project data are cached. If for any reason you make changes to test cases, test runs or tasks in the system through the database, you may need to update the cached values for test execution status and task progress that are displayed on the requirements and releases pages. To refresh the execution status or task progress data, click on the appropriate "Refresh" link illustrated above.

<u>b) Indentation Hierarchy</u>

The Requirement and Test Case pages use an "Indent" system for managing the hierarchy of information. This allows requirements and test cases to be nested under parent items and be rapidly searched and

filtered on. Sometimes if a move/copy operation is interrupted (due to a network outage, etc.) the hierarchy may get corrupted. If so, you'll see a red Error message instead of the Green OK. If that happens, just click on the appropriate "Correct…" hyperlink and the system will correct the indent levels for you.

3.2. Users

3.2.1. View / Edit Users

The following screen is displayed when you choose the "View/Edit Users" link from the Administration sidebar navigation:

This screen displays the list of users in the system (both inactive and active) together with their first name, middle initial, last name, username (login), administrative permission status and active status.

You can filter the list of users by either choosing an administrative / active status, or entering a portion of the first name, middle initial, last name or username into the appropriate text box. When you click the <Filter> button, the list of users will be filtered by the criteria you entered. You can clear the filter selection by clicking the <Clear Filters> button. To sort the list of users, just click on the appropriate arrow icon located in the header row of each field (one each for ascending / descending). In addition, the list of users is paginated into groups of fifteen (15). You can step through the different pages by clicking the page numbers at the bottom of the user list.

To add a new user to the system, simply click the <Add> button at the bottom of the user list, and a new screen will be displayed that allows you to enter the new user information:

On this screen, you can enter the name, email address and password for the new user. If you want the user to be able to subscribe to items in the system as RSS feeds, you should also make sure that the "Enable RSS Feeds" checkbox is selected and a GUID token is displayed in the text-box underneath.

In a similar way, to edit the details of an existing user, simply click the "Edit" hyperlink in the user list box, and you will be taken to the following screen that allows you modify the user details:

On this screen you can edit the first name, middle initial, last name, username, email address, system administration status and active status. Once you have made the necessary changes, click the <Update> button to commit them. If you decide that you want to ignore the changes, click the <Cancel> button and the changes will be discarded.

In addition, there are **three tabs** that allow you to add/remove the user from projects, change the user's password and update the data-mapping used when synchronizing artifacts that are assigned or created by the current user.

If you click on the "Project Membership" tab you will be shown a list of projects that the user is currently a member of:

You can change the role that the user has on the various projects, by simply choosing the appropriate role from the drop-down list and then clicking [Update]. To remove the user from a project, simply select its checkbox and then click [Delete]. To add a user to a new project, simply click on the [Add] button and then choose the project and associated role from the list of projects on the screen that is displayed:

Then click [Add] to add the selected project(s) to the user's project membership.

To change the user's password (if the user is managed by SpiraTeam) or LDAP information (if managed by an external LDAP directory server), click on the "Passwords and Security" tab:

On this tab you can either update a user's password or their LDAP Distinguished Name (DN). You can also use this screen to switch a user from LDAP-Managed mode to SpiraTeam-Managed mode.

In LDAP-Managed mode you enter the fully Distinguished Name (DN) for that user in your corporate LDAP server and provide no password. SpiraTeam® will then query your corporate LDAP server for the password information, reducing the number of passwords that a user needs to remember. Please see the sections on *"Importing LDAP Users"* and *"LDAP Configuration"* for more details.

To view/change the list of usernames that a user has in an external bug-tracking system, click on the "Data Mapping" tab. This section is used by the SpiraTeam data-synchronization service to map incidents from SpiraTeam to other bug-tracking systems

Please see the *SpiraTeam External Bug-Tracking Integration Guide* for more details on using the data-mapping tab.

3.2.1.1. Importing LDAP Users

If your organization already has an LDAP compatible user management system in place (e.g. Windows Active Directory, Novell eDirectory, OpenLDAP, IBM Tivoli, etc.), then instead of having to manually enter users one by one into SpiraTeam®, you can simply import them from your LDAP Server. Before doing this however, you need to first setup the LDAP configuration (see the section on LDAP Configuration below.

Once you have setup your LDAP server configuration in SpiraTeam®, clicking on the "Import Users From and LDAP Server" will bring up the following screen:

This screen lists all the users available in the LDAP server that have not been already imported into SpiraTeam®. The users are listed by name along with their login, email address and fully distinguished LDAP name (DN). You can narrow down the list by entering partial name matches in any of the fields displayed and clicking [Filter] and/or you can sort the results by clicking on the directional arrows in the field headings.

Select the checkbox of any users you want to import and click <Import> to complete the operation. These users can now login to SpiraTeam® and use their existing LDAP login and password information.

3.2.2. Project Membership

The following screen is displayed when you choose the "Project Membership" link from the Administration sidebar navigation:

This screen displays the name of the current project together with a list of all the users who are currently members of the project along with their currently assigned project role. If you want to modify the membership for a different project, simply click the "Change Project" link to be taken back to View/Edit Projects screen where you can select a different project.

To modify the role of a user assigned to the project, simply change the role for that user's entry in the drop-down menu and click the <Update> button. To remove a user from the project, simply check the box to the left of the user's name and click the <Delete> button. Note that this only removes them from the project, not the entire system.

To add a user to the project, so that can access its information, simply click the <Add> button and you will be taken to the following screen that lists all the users in the system that are not currently members of the project:

You now should narrow down the list of users by entering filter criteria and clicking [Filter]; you can also sort the results to make viewing easier. Once you have located the appropriate user(s), just select a project role for them from the drop-down list and click [Add] to add them to the project in the specified role.

3.2.3. Active Sessions

Often an administrator of the system will want to know how many users are currently logged into the system, especially on installations licensed by concurrent-user. Clicking on the 'Active User Sessions' administration option will display a list of all the users who currently have active sessions in the system:

Each user is displayed along with their user ID, whether they're connected through the application or via a third-party add-on, and the date they last logged-in. The administrator is able to forcibly end a user's session using the 'End Session' link to the right of their name. Clicking this link will result in that user being logged out when they try and perform an operation in the system. **Warning: You should make sure that the user is not actively using the system to prevent any unsaved data being lost**.

3.2.4. View / Edit Roles

There are six (6) default project roles that a user may be assigned to a project with:

➢ **Project Owner** – the same rights as a Manager, but in addition can access the project administration tools

➢ **Manager** – can see all screens and add/edit all artifacts, but cannot access project administration tools

➢ **Developer** – can see all screens, but can only add/edit incidents, tasks and tests and change requirement coverage

➢ **Tester** – can see all screens, but can only add/edit incidents and execute tests. Note: cannot delete incidents, only a Manager can do that.

➢ **Observer** – can see all screens, but cannot perform any write operations (insert / update / delete)

➢ **Incident User** – can only view and edit incidents. This user cannot even see the project's requirements, tasks, test cases or releases.

Note: The System Administrator is automatically added to every project as a Project Owner, and can never be removed as Project Owner, made inactive or made a different role on the project.

You can make changes to the permissions associated with each of these default roles, and also create as many additional roles as you like. To customize the roles in your installation of SpiraTeam®, simply click on the "View / Edit Roles" link in the Administration sidebar navigation:

View / Edit Roles

Role Name	Description	Active	Role #	Operations
Project Owner	Can see all screens, create/modify all artifacts, and can access the project administration tools	Yes	RX000001	Edit	Delete
Manager	Can see all screens and create/modify all artifacts, but cannot access project administration tools	Yes	RX000002	Edit	Delete
Developer	Can see all screens, but can only create/modify incidents and tests and change requirement coverage	Yes	RX000003	Edit	Delete
Tester	Can see all screens, but can only create/modify incidents and execute tests. Note: cannot delete existing incidents	Yes	RX000004	Edit	Delete
Observer	Can see all screens, but cannot perform any write operations (create / modify / delete)	Yes	RX000005	Edit	Delete
Incident User	Can only create/modify/view incidents. This role cannot see a project's requirements, test cases or releases.	Yes	RX000006	Edit	Delete

▶ Add

The screen lists all of the roles currently configured in the system (both active and inactive) together with the name, description, and an active flag. You can create new roles by clicking the <Add> button which will create a new default role entry in the list. You can edit the name, description and associated permissions of a role by clicking on the appropriate "Edit" link. You can delete an existing role, by clicking the "Delete" link. Note that you cannot delete any of the default roles, but can instead make them inactive.

Clicking on the edit link will take you to the following screen:

View / Edit Role | Tester

Please review the information listed below and make any changes if necessary.
Once you have finished, click [Update] to confirm them.

Role Name*: Tester

Description: Can see all screens, but can only create/modify incidents and execute tests. Note: cannot delete existing incidents

Project Admin*: No

Active*: Yes

Artifact Permissions

This role can perform the following operations on the various artifacts:

Artifact	Create	Modify	Delete	View
Requirement	☐	☐	☐	☑
Test Case	☐	☐	☐	☑
Incident	☑	☑	☐	☑
Release	☐	☐	☐	☑
Test Run	☑	☐	☐	☑
Task	☐	☐	☐	☐
Test Step	☐	☐	☐	☑
Test Set	☐	☐	☐	☑

Note: For Test Runs, changing the Modify, Delete and View permissions will not have any affect on the system.

▶ Update   ▶ Cancel

You can edit the name, description, project admin and active flags, and also specify the specific artifact-level permissions associated with the role. The project admin flag denotes whether this role has administration-level access to the project (for example the project owner role has this set by default). The other permissions allow you to specify if a user can create, modify, delete or view each of the artifacts in the system. If a user does not have view permissions for the artifact, then the corresponding tab in the system will also be disabled.

Note: The permission needed to <u>execute a test case</u> is the "Create + Test Run" permission since that initiates the creation of a new test run.
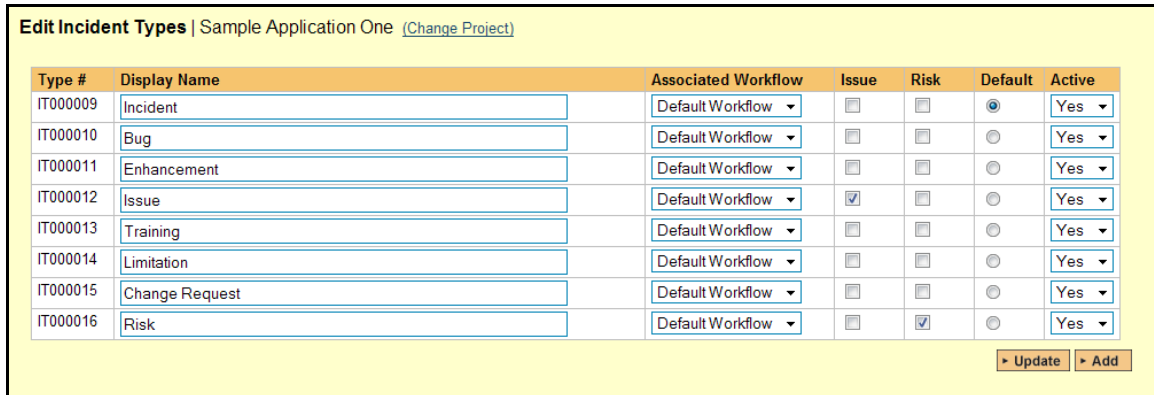
3.3. Incidents

In addition to being able to create custom properties and values for incidents (same as for all artifacts in SpiraTeam®), you can also change the values populated in many of the standard fields used in the incident tracker – types, statuses, priorities and severities. The process for changing each of these is described below:

3.3.1. Edit Types

The following screen is displayed when you choose the "Edit Types" link from the Incidents section of the administration sidebar:

The screen displays a list of all the defined incident types for the current project. By default the screen will be populated with the standard SpiraTeam® incident types. To edit an existing incident type, simply change the name, associated workflow, issue check-box, risk check-box, set a default type and/or change the active flag then click <Update>.

You can't delete an existing incident type, but to prevent it appearing in any drop-down-lists, all you need to do is change its active flag to "No" and click <Update>. To add a new incident type, click the <Add> button and a new row will be added to the list which you can now edit.

The associated workflow drop-down list allows you to specify which workflow the incident type will follow. This is a very powerful feature since it allows you to configure different workflows for different incident types; i.e. a bug may follow a workflow geared to identification and resolution, whereas a risk may only need a much simpler set of steps and actions.

The issue and risk check-boxes allow you to specify if the incident type is an issue or risk-type, which means it is would be eligible for display in the issue or risk section of the project home page respectively. The default radio button allows you to specify which incident type should be the default for newly created incidents. This is the type that a new incident will be set to unless changed by the creator of the incident. Note that you must have at least one active incident type, and you cannot set an inactive type as the default.

3.3.2. Edit Statuses

The following screen is displayed when you choose the "Edit Statuses" link from the Incidents section of the administration sidebar:

The screen displays a list of all the defined incident statuses for the current project. By default the screen will be populated with the standard SpiraTeam® incident statuses. To edit an existing incident status, simply change the name, open check-box, set it as the default status and/or change the active flag then click <Update>.

You can't delete an existing incident status, but to prevent it appearing in any drop-down-lists, all you need to do is change its active flag to "No" and click <Update>. To add a new incident status, click the <Add> button and a new row will be added to the list which you can now edit.

The open check-box allow you to specify if the incident status should be considered open or not, which means it is would be eligible for display in the various sections of the user's home page and the project home page that list open incidents. The default radio button allows you to specify which incident status should be the default for newly created incidents. This is the status that a new incident will be set to when first created, and acts as the first step in the incident workflow. Note that you must have at least one active incident status, and you cannot set an inactive status as the default.

3.3.3. Edit Priorities

The following screen is displayed when you choose the "Edit Priorities" link from the Incidents section of the administration sidebar:

The screen displays a list of all the defined incident priorities for the current project. By default the screen will be populated with the standard SpiraTeam® incident priorities. To edit an existing incident priority, simply change the name, color and/or change the active flag then click <Update>. Note that you can either enter the hexadecimal RRGGBB code for the color or use the pop-up color picker.

You can't delete an existing incident priority, but to prevent it appearing in any drop-down-lists, all you need to do is change its active flag to "No" and click <Update>. To add a new incident priority, click the <Add> button and a new row will be added to the list which you can now edit.

3.3.4. Edit Severities

The following screen is displayed when you choose the "Edit Severities" link from the Incidents section of the administration sidebar:

The screen displays a list of all the defined incident severities for the current project. By default the screen will be populated with the standard SpiraTeam® incident severities. To edit an existing incident severity, simply change the name, color and/or change the active flag then click <Update>. Note that you can either enter the hexadecimal RRGGBB code for the color or use the pop-up color picker.

You can't delete an existing incident severity, but to prevent it appearing in any drop-down-lists, all you need to do is change its active flag to "No" and click <Update>. To add a new incident severity, click the <Add> button and a new row will be added to the list which you can now edit.

3.4. Workflows

Clicking on the "Edit Workflows" link in the Administration sidebar navigation brings up the list of defined incident workflows for the current project. A workflow is a predefined sequence of incident statuses linked together by "workflow transitions" to enable a newly created incident to be reviewed, prioritized, assigned, resolved and closed, as well as to handle exception cases such as the case of a duplicate or non-reproducible incident. The workflow list screen for a sample project is illustrated below:

To modify the name, default status, notify and/or active flags, simply change the values in the appropriate text-box, radio-button, check-box or drop-down list and click the <Update> button. To add a new workflow, simply click the <Add> button and a new workflow will be created with the standard SpiraTeam® steps and transitions.

You can have as many workflows as you like in a project, but only one can be marked as the default. Each incident type is assigned to a workflow; this allows you to have different incident types follow different paths from creation of closure. However when a new incident type is created, it will be initially associated with the project's default workflow. The steps and transitions that make up the default workflow are illustrated in the diagram below:
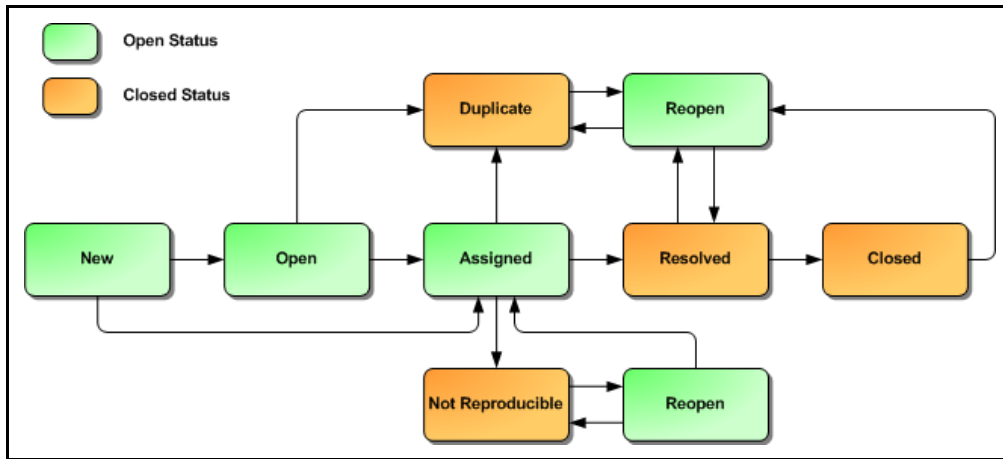
The notify flag is used to tell SpiraTeam® whether that particular workflow should have email notifications turned on or off. You define what transitions and which recipients should receive the emails in the workflow transition editor (see below), but you can globally turn on/off notifications here as well. This is useful if you find that the notifications are becoming an annoyance, or if the email server is unavailable for a period of time.

Note: You can only assign an active workflow to an incident type, and similarly you cannot make a workflow inactive that is currently linked to an incident type. This is important as all incident types need to be linked to an active workflow at all times.

3.4.1. Edit Workflow Details

Clicking on the <Steps> button of an inactive workflow brings up the following screen that lists all the workflow steps and workflow transitions that comprise the workflow:

This page lists in the left-most column all the various incident statuses defined for the project. The next column lists all the possible transitions that can occur *from that status*. In addition, with each transition is listed the name of the resulting *destination status* that the transition leads to. E.g. from the assigned status, depending on your role (see later) you can move the incident to either duplicate, resolves or not-reproducible depending on which transition the user takes.

Clicking on the name of a step or transition takes you to the appropriate details page (see below) where you can set the properties of the step or transition respectively. To delete an existing transition, simply

click the <Delete> button after the transition name, and to add a new transition, click the <Add Transition> button in the Operations column.

3.4.2. Edit Workflow Transition

When you click on the transition name link from the previous screen, you are taken to the workflow transition details screen:

The top part of the screen is the "workflow browser" which illustrates how the transition relates to the workflow as a whole. It displays the current transition in the middle, with the originating and destination steps listed to either side. Clicking on either incident status name will take you to the appropriate workflow step details page. This allows you to click through the whole workflow from start to finish without having to return to the workflow details page.

Each transition has a series of conditions which need to be satisfied for a user to actually execute the transition (i.e. move the incident from the originating status to the destination status) and a set of notification rules that allow you to specify who should get an email notification if the transition is executed. Both the conditions and notifications allow you to set three types of user role:

➤ The detector of the incident can be allowed to execute the transition, and/or be notified when the transition occurs. For example, when an incident is marked as Resolved, the detector should be the only one who's allowed to move it to Closed. Similarly when an incident is moved from Assigned to Resolved, the detector should probably be notified so that he knows to log in and verify that it has been resolved satisfactorily.

➤ The owner of the incident can be allowed to execute the transition, and/or be notified when the transition occurs. For example, when an incident is marked as Assigned, the assigned owner should be the only one who's allowed to move it to Resolved. Similarly when an incident is moved from Open to Assigned, the owner should probably be notified so that he knows to log in and begin resolving the incident.

➤ A user with a specified role can be allowed to execute the transition, and/or be notified when the transition occurs regardless of whether they are the detector or owner. For example a user with role "Manager" might want the power to close all incidents regardless of ownership status, and might also want to be notified when any incident is marked as Not-Reproducible.

You can set any of these conditions by changing the drop-down list and/or check-boxes and clicking the appropriate <Update> button.

3.4.3. Edit Workflow Step

When you click on the incident status name link from either of the previous screens, you are taken to the workflow step details screen:

The top part of the screen is the "workflow browser" which illustrates how the step relates to the workflow as a whole. It displays the current incident status in the middle, with the possible originating and destination transitions listed to either side. Clicking on either workflow transition name will take you to the appropriate workflow transition details page. This allows you to click through the whole workflow from start to finish without having to return to the workflow details page.

This page allows you to define the behavior of the various incident fields (i.e. those that are a standard part of SpiraTeam® such as Priority) and incident custom properties for this particular step in the workflow. You can set each of the fields/custom properties as being active and/or required for each step in the workflow. Note that you cannot set a field/property as being required and inactive since this would prevent a user from ever updating the incident. For example, when an incident is in the New status, you might make the owner field inactive (since a detector shouldn't need to know who will ultimately own it), when it gets to the Open status, you might make the field active, and when it gets to the Assigned status, you might make it active and required. This allows you to tailor the information gathered to the appropriate place in the workflow.

To actually make these changes, all you need to do is select the appropriate checkboxes in the list of fields and custom properties and click the corresponding <Update> button.

3.5. Notifications

This section allows the administrator and project owner to configure email server configuration, email notification content, and when notifications are sent. Server configuration and artifact templates can only be changed by the system Administrator. However, notification events can be configured by the project owner.

3.5.1 Email Configuration

The Email Configuration page is split into two sections. The first section covers email notification details, and the second section configures how email from the application is sent.

Email Configuration

By default, SpiraTeam will use the default IIS SMTP Virtual Server to send outgoing email notifications to users in the system. However, it can also be configured to send emails through an external SMTP server directly.

This page allows you to change these mail server settings as well as specify the URL that is used to access SpiraTeam when clicking on a hyperlink in an email notification:

E-Mail Notifications Active?	No
	If disabled, SpiraTeam will not send out any messages.
Web Server URL*:	http://localhost/SpiraTeam
	The base URL used to access SpiraTeam (e.g. http://myserver/SpiraTeam)
From E-Mail Address*:	administrator@mycompany.com
	The address that emails will be sent from. Replies to this address will not be monitored.
Reply-To E-Mail Address:	
	The Reply-To field that emails sent will contain. Blank will leave header field blank in messages.
Send HTML Emails?	Yes
	If enabled, emails will be sent out in HTML. Otherwise, plain text.
Allow Users Control of Receiving Emails?	Yes
	If enabled, users will be given the option to deny receiving emails from the system.

- **Email Notifications Active?** – Defaults to Yes. If changed to No, the system will not send out any emails, regardless of other settings. Note that this means that new user requests will not get sent either.

- **Web Server URL –** This is the URL that your users use to access the system. Do not put the /Login.aspx or any other page here, as this URL is used to generate links to pages in the application.

- **From Email Address –** This is the email address specified in the 'From:' field of email notifications sent from the application.

- **Reply-To Email Address –** This is the address specified in the 'ReplyTo:' field for notification emails sent from the application.

- **Send HTML Emails?** – Defaults to Yes. This option specifies whether HTML or Plain-Text emails are sent from the system.

- **Allow Users Control of Receiving Emails?** – Defaults to Yes. This specifies whether or not a user can modify their profile to not receive any emails from the system. If set to no, users' preference will be enabled and locked out.

Mail Server

Please leave all the following fields empty if you want to use the default IIS SMTP Virtual Server:

Host Name:
The SMTP host name of your mail server.

Port Number:
The SMTP port number to use. Blank to use default of 25.

SSL Connection: No ▼

User Name:
If your SMTP requires authentication, this is your username.

Password:
If your SMTP requires authentication, this is your password.

▸ Update

To use the internal IIS's default virtual SMTP server, leave all fields blank. The virtual server must then be configured to use proper SMTP server and network configuration. If you want the application to contact an SMTP server directly, use the following fields:

- **Host Name –** This is the SMTP server to connect to.

- **Port Number –** This is the port number to use, blank uses the default port 25.

- **SSL Connection –** Whether or not to use an SSL connection with the server. Be sure that the SMTP server's SSL certificate is trusted on the application server.

- **User Name –** When using an authentication method, this is the username to log in as.

- **Password –** When using an authentication method, this is the password to use.

Example settings for connecting to Gmail/Google Mail for sending notifications:

- ❖ **Host Name:** smtp.gmail.com

- ❖ **Port Number:** 587

- ❖ **SSL Connection:** Yes

- ❖ **User Name:** <account>@gmail.com

- ❖ **Password:** <account password>

3.5.2 Notification Templates

Notification templates are used by notification events, and are defined system-wide for each artifact type.

Notification Templates

Here you can specify the e-mail notification templates sent out for each Artifact type. To edit the template, select the Edit Template link.

To send a test e-mail using the template, select the Test Template link. The test e-mail will be sent using the first item in the project.

Artifact Type	Prefix	Operations
Requirement	RQ	Edit | Test
Test Case	TC	Edit | Test
Incident	IN	Edit | Test
Task	TK	Edit | Test
Test Set	TX	Edit | Test

To edit a template, click the Edit link. To send a test email notification to yourself using the specified template, click the Test link.

Clicking the Edit link will take you to a page similar to the following. Depending on the artifact type you selected, the list of available fields will vary.

Notification Templates | Return to Template List

The template below will be sent whenever an event is matched for an artifact Requirement. Tokens in the template will be substituted when an e-mail is set. Otherwise, the template will be sent as-is to assigned users and roles.

${Product}
Requirement: ${Name} (${ProjectName})
${Description}

▸ Update   ▸ Cancel

The following are all available tokens for Requirements and their meanings. Tokens not in this list will be taken out of the final message. Click on a token to insert it into the current cursor position in the editor above.

${Author}	The name of the Author	${Comments}	Currently not used.
${Description}	Descriptive text	${EventName}	The name of the event that fired the notification.
${ID#}	The ID# of the item.	${Importance}	The current Importance
${Name}	Name of the Requirement	${NotifyTo}	The notification receiver's name.
${Owner}	The name of the Owner	${PlannedEffort}	Planned effort in HH:MM
${Product}	The name of the application.	${ProjectName}	The name of the project.
${Release}		${ScopeLevel}	The current Status
${TaskActualEffort}	Assigned Task's actual effort in HH:MM	${TaskEstimatedEffort}	Assigned Task's planned effort in HH:MM
${TaskProjectedEffort}	Assigned Task's projected effort	${TaskRemainingEffort}	Assigned Task's remaining effort
${URL}	URL to link to artifact.		

On this screen you are presented with the same rich text editor available elsewhere in the application. Displayed in it is the current template (with template tags showing) for the artifact. Template tags start with a $ (dollar sign) and then a string name enclosed in () parentheses. When email notifications are sent, tokens will be replaced with specific information from the artifact that the notification is being sent

for. Invalid tokens will be stripped from the template text. Clicking a token in the list will insert it in the current position in the textbox for easy selecting and editing.

If HTML notifications are disabled, the template will be converted to plain text before sending.

When finished, click the update button to save your new template. The new template will take effect immediately.

3.5.3 Notification Events

The Notification Events section is where project managers can set up when and to whom notifications are sent out to users of the system. Clicking on the Notification Event link will present you with a list of all events defined for the current project:

Note: These events can handle all changes to any of the artifacts except changes handled by Status changes to Incidents. Incident status changes are handled through the Workflow configuration.

When clicking on the Edit link or Add button, you will be presented with the event details screen:

Notification Event Details | Incident: Owner Assigned

<u><< Back to Notification Event List</u>

Event details are listed below. You can edit the fields and users and wither or not this event is fired on creation, but once created the Artifact Type cannot be changed.
Once finished, click [Update] or [Insert] to save your changes.

Event Name: `Incident: Owner Assigned`

Artifact Type: `Incident ▼`
This event will be attached to this artifact type.

On Creation? `No ▼`
Whether this event is fired on a new artifact creation.

Active? `Yes ▼`
Whether this event is active or not.

Subject Line: `${Product} - Incident ${ID#} has been assigned to you.`
The subject-line of the e-mail notification. Tokens used in the email template can be used in the subject line.

The top section defines general configuration items for the event:

- **Event Name:** used to name the event, only used for administrative purposes.

- **Artifact Type:** The artifact type this event is attached to. Once an event is created, the artifact type cannot be changed.

- **On Creation?** If set to yes, this event will fire when an artifact is created, as well as when any configured fields are changed.

- **Active?** If set to yes, this event is active and will send notifications when configured fields are modified.

- **Subject Line:** The subject line of the notification email.

The Artifact Fields will let you configure which fields will cause this notification to send an email notification:

Artifact Fields:
This event will be active if any of the selected fields are changed.

Field	Notify On Change?
Severity	☐
Priority	☐
Type	☐
Detected By	☐
Owned By	☑
Detected Release	☐
Resolved Release	☐
Verified Release	☐
Name	☐

Selected fields are treated in an OR-based query, so that if you have two or more fields checked for an event, the event will send a notification if **either** of the two fields are changed. Depending on the artifact type configured above, the available fields will vary.

The last section is the configuration of whom to send the notifications to:

Users and Project Roles:
When a selected field is changed, the following users or roles will be notified.

User / Project Role	Enabled?
Artifact Opener or Creator:	☐
Artifact Owner:	☑
Project Roles:	
Project Owner:	☑
Manager:	☐
Developer:	☐
Tester:	☐
Observer:	☐
Incident User:	☐

If a user belongs to more than one group or they have manually signed up to receive notifications to any changes in the artifact, they will only receive one notification for the artifact change.

3.6. Documents

SpiraTeam® includes a built-in web-based document management system that allows you to upload and share documents between project team members. These documents are stored in folders, categorized by a series of user-defined meta-tags and can also be associated with other artifacts in the system (e.g. requirements, incidents, etc.).

The set of administrative options located under the "Documents" heading allow the Project Owner to configure how the documents are organized in their particular project.

3.6.1. Edit Document Types

When users upload documents into a SpiraTeam project, they are required to specify the type of document that is being uploaded. The list of document types is configurable by the Project Owner for each individual project.

When you click on Documents > Edit Types, you can edit the list of types available:

By default, each project will be created with a single document type called 'Default'. You can add additional document types and/or change the name of the ones already created. If you decide that you no longer want to use a specific document type, you can set its active flag to "No".

The only requirement is that each project needs to have at least one active document type available, and that there is one active type designated as the default type. The default type is the option that will be initially selected when a user uploads a file / URL to the project.

3.6.2. Edit Document Folders

In addition to associating the documents in the system with a "document type", they can also be organized into a hierarchy of folders. Clicking on Documents > Edit Folders allows the Project Owner to create / modify the folder structure into which users can upload the documents for sharing and collaboration:

Initially, new projects are created with a single folder called "Root Folder", under this folder, you can click the [Add] button to add additional folders, "Edit" to change the name and/or location of an existing folder, or "Delete" to permanently remove a folder. *Note that deleting a folder will remove all its subfolders and any documents contained in the folder and subfolders.*

When you click on either [Add] or "Edit", you will be taken to the following screen that allows you to edit the details of the new/modified folder:

The first field allows you to specify the name of the folder as it will be displayed to users in the system, and the second field allows you to tell the system which parent folder should contain the new folder. You cannot make the root folder a child of an existing folder, and there can only be a single root folder per project.

3.7. Custom Properties

SpiraTeam allows you to customize all of the artifacts in the system (requirements, test cases, incidents, etc.) by adding user-defined custom properties in addition to the built-in fields. You can create either *text* properties that a user needs to enter in a text-box, or *list* properties that the user can choose from a drop-down-list.

3.7.1. Edit Custom Lists

If you are planning on having any list based custom properties in your project, then you first need to create and populate the custom project lists that the user will be able to select from. These lists are stored separately from the individual artifact types so that you can have one set of values (e.g. list of operating systems under test) be reused by multiple artifact types.

The following screen is displayed when you choose the "Edit Custom Lists" link from the Administration sidebar navigation:

The screen displays all the custom lists currently defined within the project, together with an active flag. By default the screen will initially be empty so the first thing you need to do is click <Add> to create a new custom list. After changing the name, just click <Update> to commit the change.

Once you have all the project lists defined, you should then click on the "Edit Values" link to display the list of values associated with the list. This is the set of values that the user will select from the drop-down list when the custom property is displayed:

Edit Custom List Values | Operating System

<< Back to Custom Lists

The following custom values have been created for this list. Please make any changes and click [Add] or [Update].
To remove an existing custom list value just make it inactive by setting its Active flag to No.

Value #	Display Name	Active
PV000009	Windows 2003	Yes
PV000010	Windows Vista	Yes
PV000011	Windows XP	Yes
PV000012	Windows 2000	Yes
PV000013	Windows NT 4.0	No

▸ Update ▸ Add

To add a new custom list value, click the <Add> button and a new row will be added to the list which you can now edit. To edit an existing custom list value, simply change the name in the textbox and click <Update>. You can't actually delete an existing custom list value, but to prevent it appearing in any drop-down-lists, all you need to do is change its active flag to "No" and click <Update>.

3.7.2. Edit Custom Properties

This link is used to actually setup the custom properties associated with each artifact type in the project. The following screen is displayed when you choose the "Edit Custom Properties" link from the Administration sidebar navigation:

The screen displays a list of all the possible custom properties for a particular artifact type for the current project. Each artifact type (requirement, test case, etc.) can have up to ten (10) custom text properties and up to ten (10) list properties. The text properties are ones where the user can enter any textual data they like, so typically it is useful for notes, comments and other freeform fields where the range of inputs is not known ahead of time. The list properties are ones where you want the user to pick the value from a predefined list of options defined by you ahead of time.

Initially the screen will default to showing the existing custom properties for a project's Requirements; to change the list to a different artifact type (e.g. Incidents), all you need to do is change the artifact type in the drop-down-list. This will refresh the list to show the custom properties for that artifact type.

To add a custom property to an artifact, all you have to do is enter an alias name for the custom property from one of the twenty (20) available entries in the list and click the <Update> button. For list properties you also need to choose the name of a matching custom list that has been defined for this project.
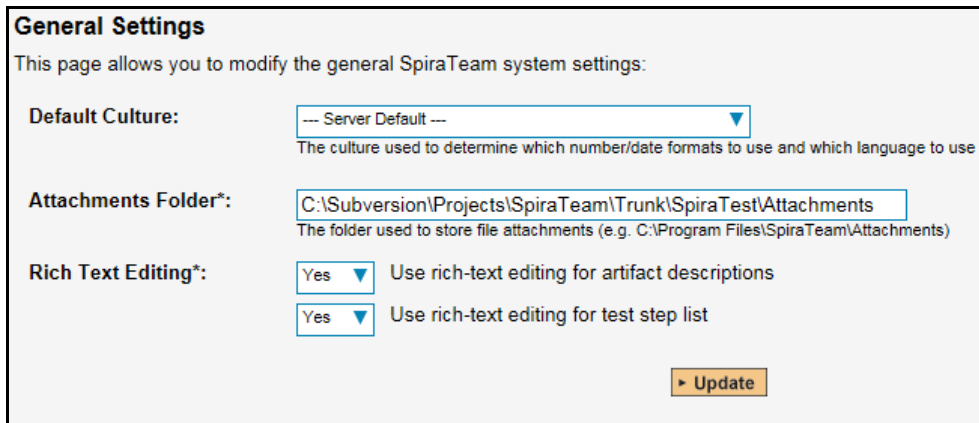
Any entry that has a defined alias will be displayed on that artifact's details page. To remove an existing custom property for an artifact, again all you need to do is click on the alias text box for that entry and delete the name of the property, then click <Update>. The system will automatically insert entries for newly added aliases and delete entries for those whose aliases are removed.

3.8. System

3.8.1. General Settings

The general settings page allows you to configure SpiraTeam® to better match your environment and setup. In the current version, you can specify the default language, configure the folder used to store document attachments and also the type of text editing for the longer, descriptive text fields used in the application (e.g. a test case's description):

Default Culture – SpiraTeam can display information in a variety of different languages (assuming that the appropriate language packs have been installed) and number formats. By default, SpiraTeam will use the regional settings (language and number formats) of the operating system it has been installed on. However, you can override this default by choosing the appropriate culture from the list of options displayed in the drop-down list. *Note: The list of culture options does not reflect the available language packs, so in some cases, the setting will only change the number formats.*

Attachments Folder - By default when SpiraTeam® is installed, the document attachments uploaded in the system get stored inside the C:\Program Files\SpiraTeam\Attachments folder located inside the main SpiraTeam® installation root. However you may want to have the documents stored on a remotely mounted drive or on a different hard disk partition. In which case you can simply change the folder pointed to in the text-box illustrated above and then click [Update] to commit the change.

Rich Text Editing - When editing certain text fields inside the system, the user is presented with a 'rich-text' interface that allows them to set the formatting of the text using a toolbar:
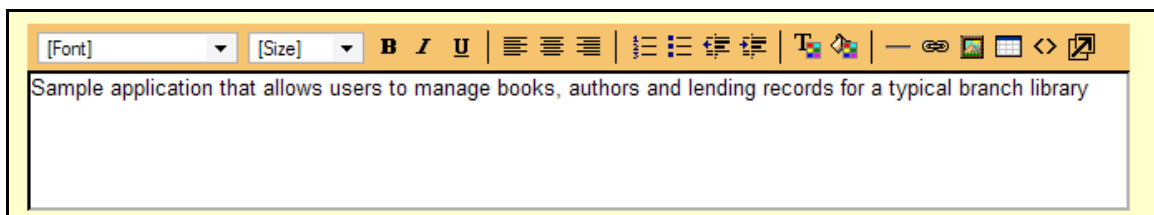
In addition this toolbar includes the option to insert bulleted lists, tables, links to other websites and other text effects. However this functionality can cause certain pages in the application to load more slowly on some browsers (e.g. Internet Explorer 6.0 or earlier) – especially on the test case details screen, which has rich-text editors for each of the test steps.

If you experience performance issues, you can use the configuration options on this page to turn off rich-text editing for just the test steps (which causes the most performance issues) or for both the test steps and for the various other description text-boxes. You can change this setting at any time, but any existing

formatted text will appear as HTML markup if you switch from rich-text to back to plain-text on an existing installation.

3.8.2. License Details

The license details page displays the information about the installed license for the particular instance of SpiraTeam® being used. The information displayed includes: the product name (e.g. SpiraTeam), the license version (e.g. v1.0.0.0), type of license in effect (x-user fixed, x-user concurrent, demonstration, enterprise, etc.), the organization that the license belongs to, the actual license key code and finally the number of users concurrently logged-in. This last piece of information is useful as it helps administrators track down how many licenses are currently in use.

A sample page is illustrated below:

To change the license key used by the system (for example, if to upgrade from Trial edition to Standard edition), you do **not** need to reinstall SpiraTeam®. All you need to do is simply change the information in the **organization** and **license key** text-boxes to match the license key and organization name found in the customer area of our website (http://www.inflectra.com/CustomerArea) and click the <Update> button.

If there is an issue with the license key (e.g. a trial version that is passed its expiration date, or where the license key doesn't match the organization name) an error will be displayed describing the specific issue with the information you entered. If you are unable to get the system to work with the license key information, please contact Inflectra® customer support at: support@inflectra.com.

3.8.3. LDAP Configuration

As described previously, you can configure SpiraTeam® to use an external LDAP server for importing new user profiles into the system, and for authenticating users – instead of having to store separate passwords inside SpiraTeam®. However you need to first configure the LDAP server settings. To do this, click on the "LDAP Configuration" link the Administration navigation:

You need to fill out the various configuration settings for your LDAP server, each of which is explained in more detail below:

> **LDAP Host**
> This should contain the name of the LDAP server that you want SpiraTeam to connect to together with the port number if it's not the default of 389.

> **Use Secure Sockets Layer (SSL)**
> You should select this check-box if your LDAP server requires use of the LDAPS secure protocol. Leave unchecked for unencrypted LDAP communication.

> **Base DN**
> This should be the distinguished name of the object inside your LDAP server that contains the list of user accounts. This varies by the type of LDAP server, please consult your LDAP server documentation for more details.

> **Bind DN**
> This should be the distinguished name of the user inside your LDAP server that will be used to authenticate against when importing users. If not provided, SpiraTeam® will try and authenticate with the LDAP server anonymously.

- ➤ **Bind Password**
  The is the password of the user specified in the Bind DN field above.

- ➤ **Login Attribute**
  When SpiraTeam® imports users from the LDAP server it needs to know the user attribute inside the LDAP server that it should use to generate the SpiraTeam® user-name. For most LDAP servers the appropriate attribute would be "uid". However for Windows ActiveDirectory, the attribute "sAMAccountName" should be used instead.

- ➤ **First Name Attribute**
  Providing this optional attribute will allow SpiraTeam® to automatically populate the first name field of the imported user instead of simply using the username as a placeholder.

- ➤ **Last Name Attribute**
  Providing this optional attribute will allow SpiraTeam® to automatically populate the last name field of the imported user instead of simply using the username as a placeholder.

- ➤ **Middle Initial Attribute**
  Providing this optional attribute will allow SpiraTeam® to automatically populate the middle initial field of the imported user instead of simply leaving it blank.

- ➤ **Email Address Attribute**
  Providing this optional attribute will allow SpiraTeam® to automatically populate the email address field of the imported user instead of simply using the username@spiratest.com as a placeholder.

- ➤ **Sample User**
  You can optionally enter a sample user and password to test that the user is correctly authenticated against the server. You can update the LDAP configuration without setting this, but if you do provide a sample user/password, it will not save the configuration unless the authentication succeeds. If you choose to enter it, the user's name should be the fully-distinguished name of the user (e.g. CN=Sample User, CN=Users, OU=Headquarters, DC=MyCompany, DC=Com).

3.9. Integration

3.9.1. Data Synchronization

SpiraTeam® is capable of synchronizing its data with a variety of other systems, including but not limited to requirements management systems and standalone bug-tracking tools. The various integration plug-ins for SpiraTeam® and the steps for configuring the data-synchronization settings are described in the *SpiraTest Migration and Integration Guide*.

If you are synchronizing data between SpiraTeam® and one of these other systems, you can click on the 'Data Synchronization' administration page at any time and view a list of all the data-synchronizations taking place, together with the status and date/time of last synchronization:

In the example above, we have four plug-ins active, with incidents being exported into JIRA, Bugzilla, FogBugz and Microsoft Team Foundation Server. The data of last sync and the status indicate if there are problems with the plug-in.

The 'Refresh' link allows you to refresh the status of the page to ensure that you are seeing the most up to date information. In certain circumstances you may want to reset the date of last sync and force a particular plug-in to examine all the records in the system to see if any were not synchronized - clicking on the 'Force Complete Re-Sync' will achieve this. The recommended procedure for forcing a re-sync is to temporarily stop the SpiraTeam Data-Sync background Windows service, click the button to reset the last-sync date, and then start the service. This will ensure that the resetting doesn't happen mid-sync.

3.9.2. Version Control Integration

SpiraTeam® is capable of integrating with a variety of Version Control (VC) / Software Configuration Management (SCM) tools such as Subversion, CVS and SourceSafe. This allows you to browse the source code repositories using the SpiraTeam web interface, and more importantly link revisions in these tools to artifacts in SpiraTeam. This provides the end-to-end traceability from code commits/check-ins to the tasks, incidents and requirements that necessitated the code change.

The information on using the various version control providers for SpiraTeam® and the steps for configuring the provider-specific settings are described in the *SpiraPlan/Team Version Control Integration Guide*.

To configure a version control provider, you need to click on the Administration > Integration > Version Control link in the Administration navigation to bring up the list of configured version control providers:

By default the only provider listed will be the TestVersionControlProvider which is used for demonstration purposes only, and can be deleted from a production system by clicking on the "Delete" link to the right of it.

To add a new version control provider, click the "Add" button to enter the Plug-in details page. The fields required are as follows:

- o **Name**: The name of the version control provider that you're adding. This needs to match the name of the Plug-in DLL file that you're using (see the *SpiraPlan/Team Version Control Integration Guide* for more details on your specific tool)

- o **Description**: The description is for your use only, and does not affect operation of the plug-in.

- o **Active**: If checked, the plug-in is active and able to be used for any project.

- o **Connection Info**: This field holds the root of the repository for any project accessing the plug-in, unless overridden in the Project Settings. Use the syntax that is described for your tool in the *SpiraPlan/Team Version Control Integration Guide)*

- o **Login / Password**: The user id and the password of the user to use while accessing and retrieving information from the version control system.

- o **Other Fields**: The other fields (Domain, Custom1 – Custom5) are provider-specific and will be described in the appropriate section of the *SpiraPlan/Team Version Control Integration Guide.*

- When finished, click the "Insert" button and you will be taken back to the Version Control integration list page, with new provider listed as an available plug-in:

To edit the settings for an existing version control provider, just click on the "Edit" link next to the name of the provider and you will be able to edit the same settings that were shown above when you first created it.

Now, you may want to change some of the settings on a per-project basis. For example you may have different repositories that you want to link to each project. You still enter the base settings for the provider as illustrated above, but then you can override specific settings for each project.

To do this, click on the ">Project Settings" hyperlink next to the provider in question:

The first thing you need to do (regardless of whether you'll be overriding any of the settings) is to make the provider active for the current project. To do this, change the drop-down list to "Yes" and click [Update]:

Now you can decide whether you want to override any of the default settings for this project. Any field left blank will automatically get its settings from the default values entered earlier. In the example above, we have specified a project-specific repository path, login and password. Once you have correctly configured the project, click [Update] to commit the changes.

You are now ready to use SpiraTeam® in conjunction with the version control tool you selected. For details on how to use the Source Code integration features of SpiraTeam, please refer to the *SpiraTeam® User Manual*.

3.9.3. Test Automation

SpiraTeam® can be used to manage the development, scheduling and execution of automated unit, functional and load tests written using a variety of test automation engines (e.g. HP QuickTest Pro, SmarteScript, TestComplete, etc.). This section allows you to configure the different engines that are available in your environment so that the testers know which tools they can use to schedule tests with.

The information on using the various test automation engines for SpiraTeam® and the steps for configuring the engine-specific settings are described in the *SpiraTest/Team Automated Testing Integration Guide*.

To configure a test automation engine, you need to click on the Administration > Integration > Test Automation link in the Administration navigation to bring up the list of configured test automation engines:

To add a new test automation engine, click the "Add" button to enter the Automation Engine details page. The fields required are as follows:

- o **Name**: The name of the test automation engine that you're adding. This can be set to any name of your choice that would make sense to your users.

- o **Description**: The description is used for any comments or additional information that you need to use to describe the automation engine.

- o **Active**: If checked, the automation engine is active and able to be used in any project.

- o **Token:** This needs to match the name of the Automation Engine DLL file that you're using (see the *SpiraTest/Team Automated Testing Integration Guide* for more details on your specific tool) for the specific automation engine.

- When finished, click the "Insert" button and you will be taken back to the test automation engine list page, with new automation engine listed.

To edit the settings for an existing test automation engine, just click on the "Edit" link next to the name of the engine and you will be able to edit the same settings that were shown above when you first created it.

Edit Engine | Quick Test Pro

<< Back to Test Automation Engine Home

Please enter/edit the following information for the test automation engine. Required fields are indicated in **bold**:

Name*: Quick Test Pro

Description: Engine that integrates with HP/Mercury Quick Test Pro

Token*: QTP

☑ Active

▸ Update   ▸ Update & Close

Once you have made the appropriate changes, click the [Update] button to commit them.

You are now ready to use SpiraTest® / SpiraTeam® in conjunction with the test automation engine you added. For details on how to use the test automation features of SpiraTeam, please refer to the *SpiraTeam® User Manual*.

3.9.4. Add-Ons and Downloads

In addition to the web interface that is typically used to interact with SpiraTeam®, there are a variety of downloadable tools and extensions that allow SpiraTeam® to be used in conjunction with other applications, and also to enable the migration of data from other systems into SpiraTeam®.

To view the list of available add-ons and downloads, simply click the "Add-Ons and Downloads" link in the Administration navigation sidebar and you will be taken to the page on the Inflectra® website that lists the various add-ins for the system, together with links to the appropriate documentation.

4. Appendices

4.1. Appendix A – Troubleshooting

If you receive the dreaded "IIS 500 Internal Error" or the "Server Application Not Available" webpage when you try and access SpiraTeam® for the first time, there can be a myriad of causes. However a good first place to look for the cause is inside the Windows Event Viewer, which stores all errors raised in the system.

To open the Event Viewer, click Start > Settings > Control Panel > Administrative Tools > Event Viewer. This will open up the event viewer:
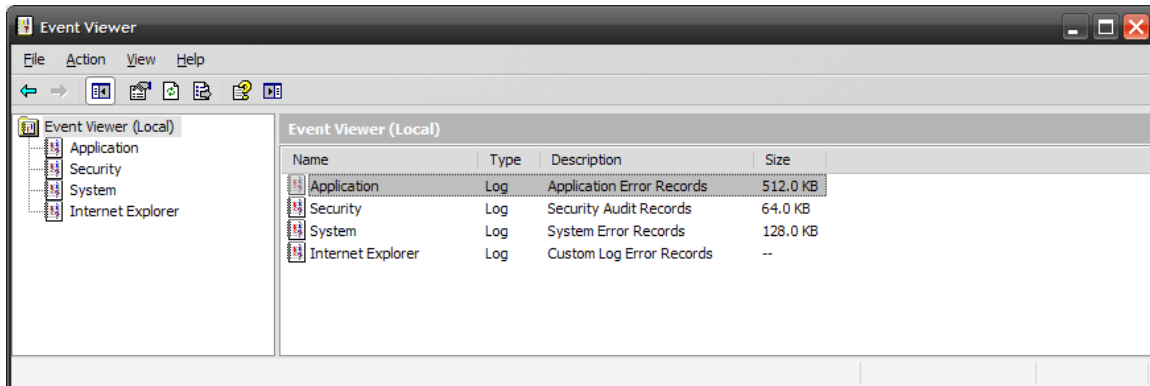
Click on the Application and System folders in turn and look for errors raised by "MSSQLSERVER", "SpiraTest", "SpiraTest DataSync Service", "DCOM", "ASPNET" or "IIS". Click on the error message, and copy the text of the message into a text editor (e.g. Notepad).

Before contacting Inflectra® customer support with the specific error message, here are a couple of common causes for the above errors together with the appropriate resolutions:

➤ **The ASP.NET process account has been disabled**
   Go to Start > Control Panel > Administrative Tools > Computer Management and launch the Windows computer management console. Expand Local Users and Groups > Users and then double-click on the 'ASPNET' account. Make sure that the ASPNET user is not disabled.
   If you are using Windows 2003 or 2008 Server the ASPNET user is set per-application pool and typically is set to the built-in NETWORKSERVICE account, so this won't apply.

➤ **The ASP.NET process account does not have sufficient permissions**
   Right-click on the C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319 folder (and any other versions of .NET that are listed) and make sure that the ASPNET, NETWORKSERVICE and LOCALSERVICE accounts are all listed with Full Control. If that doesn't fit the issue and you are using Windows 2003 or 2008 Server, open up the IIS manager and right-click on the Application Pool that SpiraTeam® is running under and make sure that the identity listed has Full Control permissions on the same folders.

➤ **The Windows Event Log is full**
   Open up the Application and System event logs, right-click on the log name and choose Properties. Make sure that both are set to "overwrite events as needed". If they are not set to overwrite as needed, change the setting then manually clear both logs.

If the resolutions above were not able to resolve the issue, please send an email to support@inflectra.com and include the error message from both the web page and the Windows Event Logs.

4.1.1. Missing MSDTC Issue

There is one common error that has been found with installations where Microsoft SQL Server was installed *after* IIS was installed. This typically affects only Windows XP Professional, but could occur in other situations. What happens is that the SQL Server installation inadvertently removes the *Microsoft Distributed Transaction Coordinator* (MSDTC) service from the system during the installation.

To determine if this is indeed the cause of the observed error, you need to click on Start > Settings > Control Panel > Administrative Tools > Component Services:
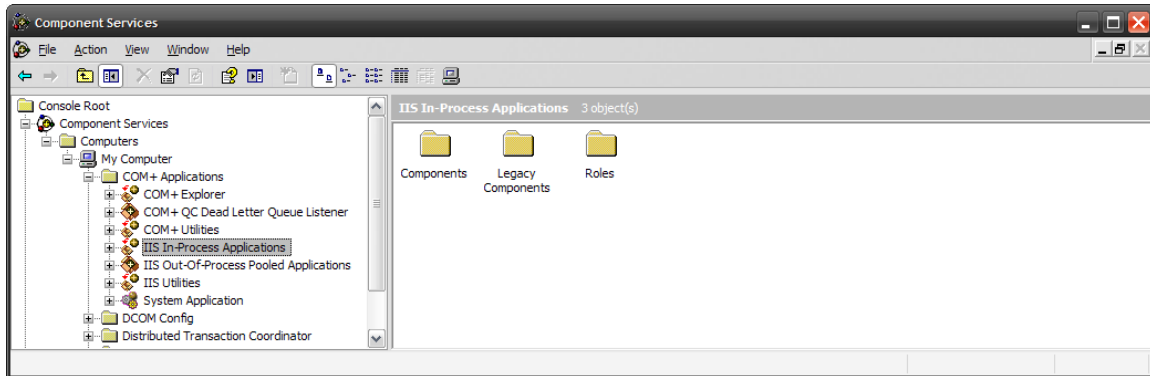
Once the window has opened, expand the folders marked "Component Services", "Computers", "My Computer" and "COM+ Applications" in turn. If the window opens correctly and displays the information illustrated above, then your IIS 500 error is being caused by something else.

However if you receive an error message that indicates an inability to connect with the "Distributed Transaction Coordinator", then you have to fix the MSDTC service to enable IIS and ASP.NET to operate properly.

To fix the issue, you need to make changes to the Windows System Registry (hereafter referred to as "the registry"). This is a process that should **not** be attempted by novice users, since any incorrect changes can complete wreck the Windows installation, requiring a complete reinstallation of the operating system.

To open the registry, click Start > Run, and type "Regedit.exe" into the dialog box, and the registry will open:
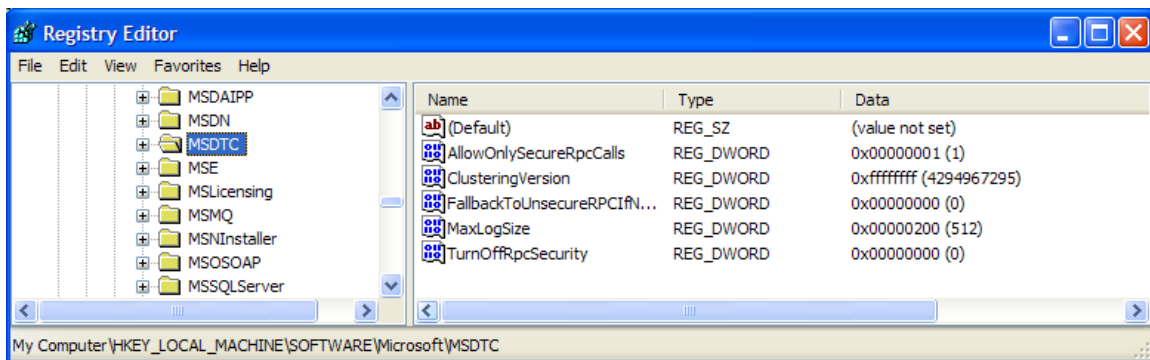
Expand the folders marked "My Computer", "HKEY_LOCAL_MACHINE", "SOFTWARE" and "Microsoft" in turn and navigate to the folder marked "MSDTC". Click the <Delete> button on your keyboard, and click <OK> on the confirmation box. Now close the registry editor.

Now you need to click on Start >Settings > Control Panel > Add or Remove Programs and click on the tab marked "Add/Remove Windows Components":
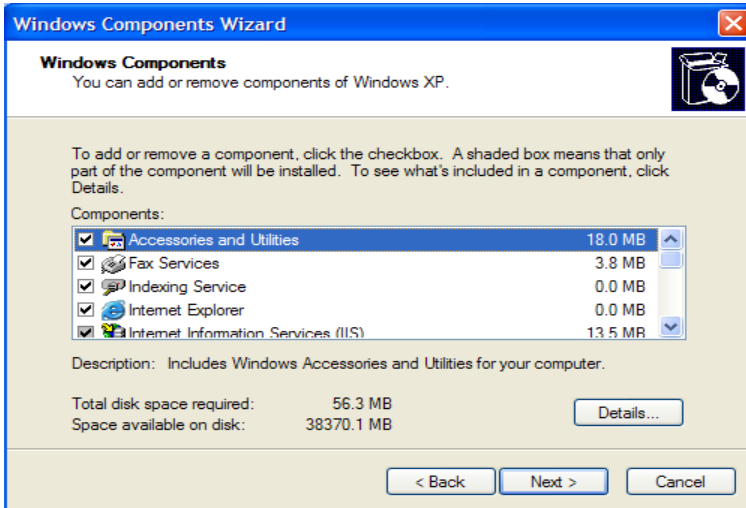
Don't change any of the selected components, but instead simply click the <Next> button. The Windows installer will detect that the MSDTC is missing (due to the registry change you made) and will now reinstall it correctly. Once this has finished, reboot the system and you should now be able to access ASP and ASP.NET applications from within IIS.

4.1.2. Application Session Pooling Issues (Windows 2003)

This issue can affect Windows Server 2003 using IIS 6.0. Since the 6.0 release of IIS, there is the ability to separate the web-server into different "Application Pools". Sometimes, web hosting companies will host multiple websites in the same application pool (which we do not recommend). When resources are maxed out for an application pool IIS 6 starts to recycle these sites causing application variables to be lost for those recycled sites. *By default, SpiraTeam installs on these operating systems in its own application pool.*

If you are experiencing application/session loss symptoms then we recommend asking your web hosting company to verify that your instance of SpiraTeam is running in its own application pool with all recycling options disabled and the recycle worker process set to recycle only once during the day at a set time.

To make these changes yourself, you need to follow these steps:

1) Add new application pool for "SpiraTeam" if one does not already exist:
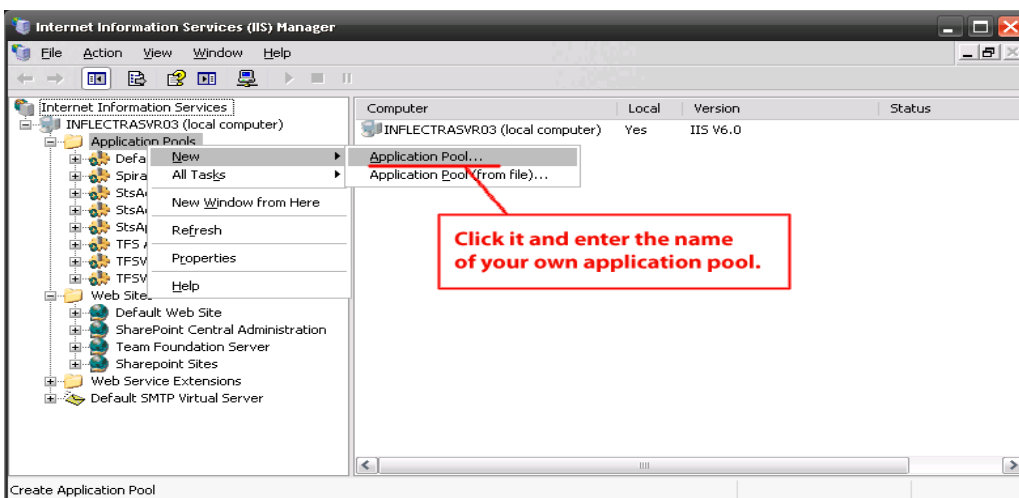
2) Next, choose your own application pool in the SpiraTeam web site properties:
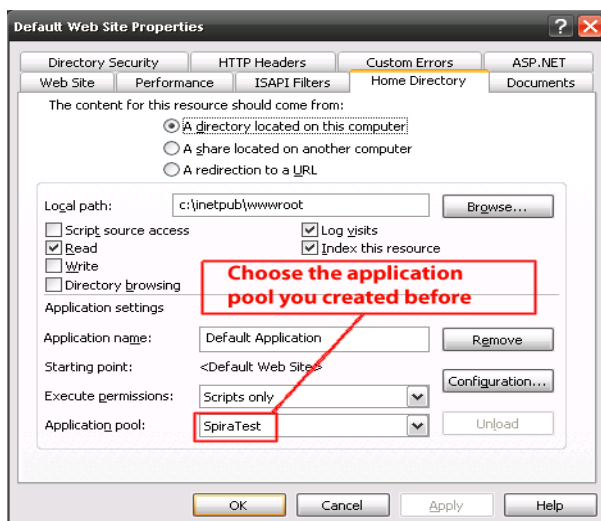
Click <OK> and you should now find that the issues with sessions disappearing has been corrected.

4.1.3. Application Session Pooling Issues (Windows Vista, 7 or 2008)

This issue can affect Windows Vista, 7 or Server 2008 using IIS 7.0. Since the 6.0 release of IIS, there is the ability to separate the web-server into different "Application Pools". Sometimes, web hosting companies will host multiple websites in the same application pool (which we do not recommend). When resources are maxed out for an application pool IIS 7 starts to recycle these sites causing application variables to be lost for those recycled sites. *By default, SpiraTeam installs on these operating systems in its own application pool*.

If you are experiencing application/session loss symptoms then we recommend asking your web hosting company to verify that your instance of SpiraTeam is running in its own application pool with all recycling options disabled and the recycle worker process set to recycle only once during the day at a set time.

To make these changes yourself, you need to follow these steps:

Add new application pool for "SpiraTeam" (if one does not already exist) and make sure it is set to use the .NET Framework v4.0 and the "Integrated Pipeline":
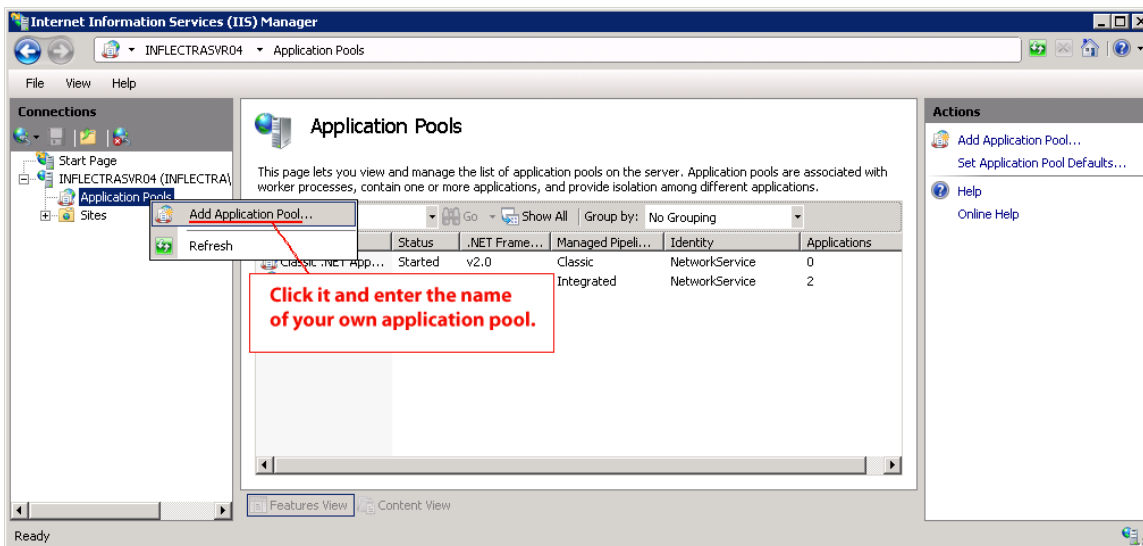
Next, choose your own application pool in the SpiraTeam web site properties:

Choose the application pool you created before
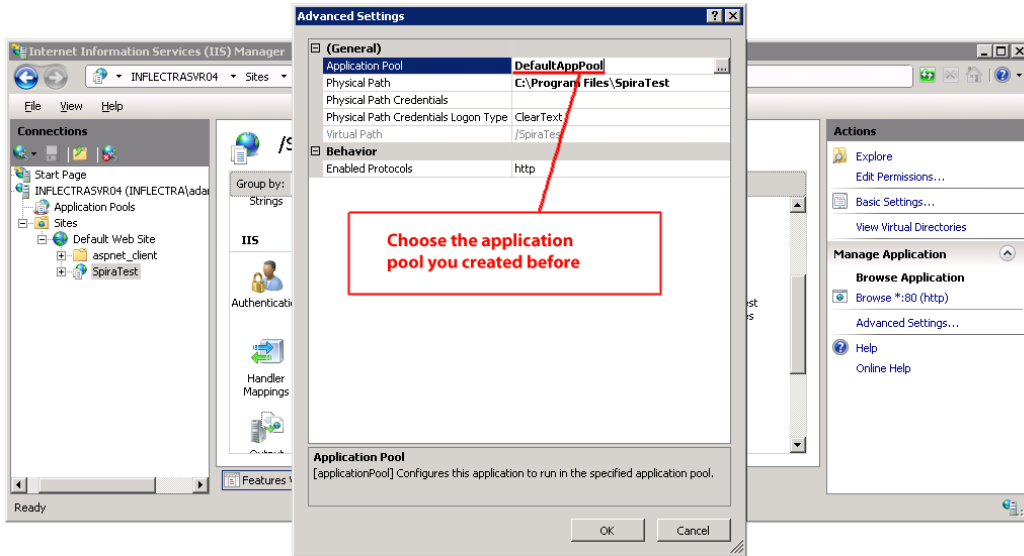
4.2. Appendix B – Using with SSL

This section outlines how you can install a Secure Sockets Layer (SSL) certificate onto IIS to allow users to access SpiraTeam® via an encrypted protocol, so that usernames, passwords and sensitive project data cannot be "sniffed" across the network. This is especially important if your web-server is being accessed across the Internet.

This section assumes that you already have a Certificate Authority (CA) available to generate an SSL certificate for you. This can either be a third-party provider (e.g. Verisign) or a tool used to generate "self certificates" that can be used internally to your organization (e.g. the IIS Certificate Server that ships with Windows Server 2003 or 2008). For more information on the differences between these two options, please read the following documents:

http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/8d3bb71a-0a7f-443f-8084-908d0dab9caa.mspx?mfr=true (installing self or third-party certificate on Windows Server 2003)

http://www.somacon.com/p42.php (installing self-certificate on Windows XP)

Once you have decided how you will generate the certificate, you next need to generate the request for the certificate from your web server. First, click Start > Settings > Control Panel > Administrative Tools > Internet Information Services to bring up the IIS management console:
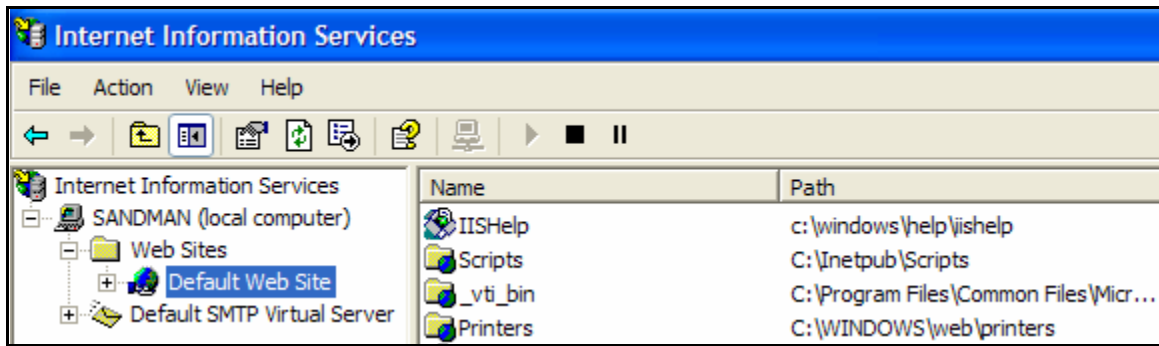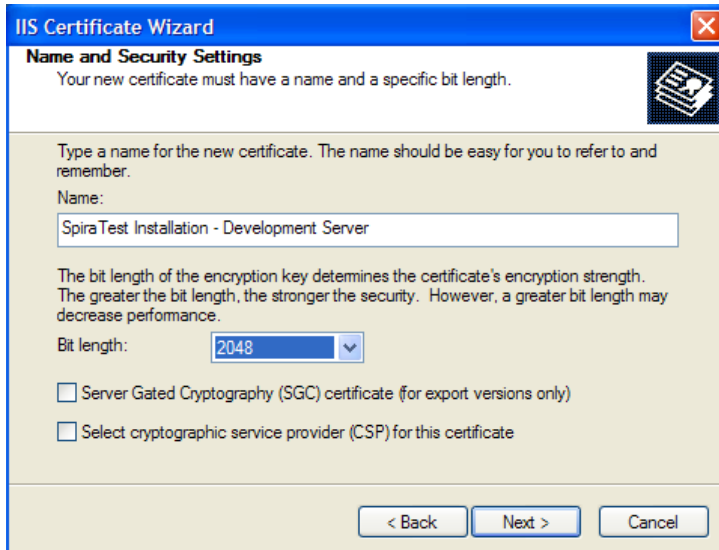
Now, right-click on the "Default Web Site" and choose "Properties", then click the "Directory Security" tab:
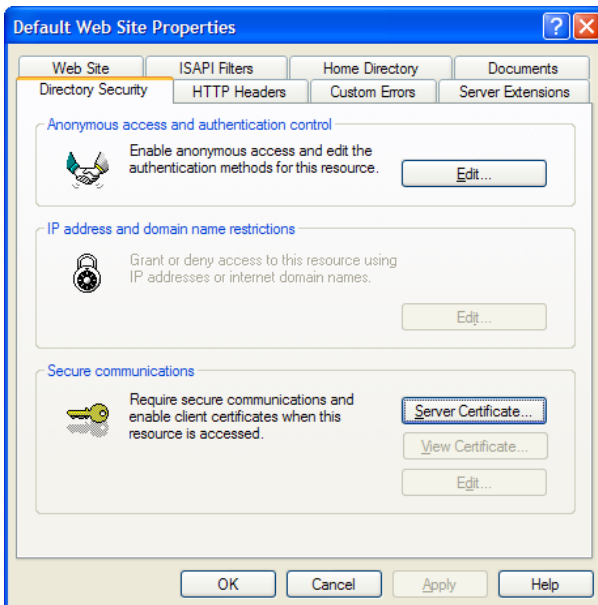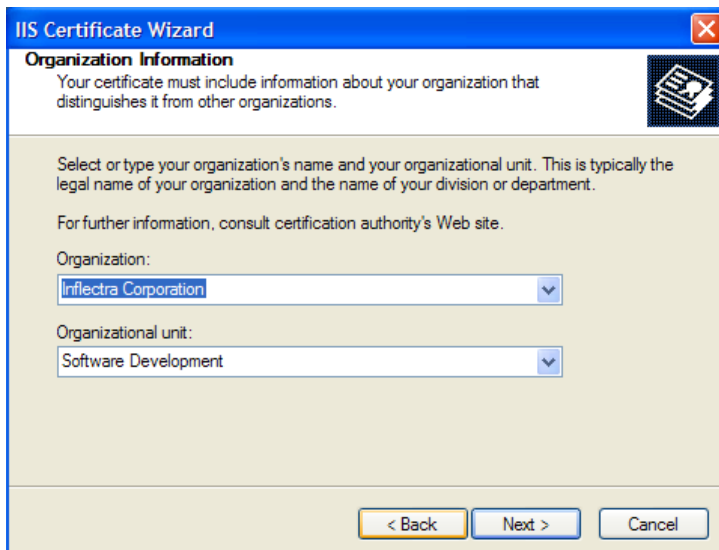
Now, click the button marked "Server Certificate", click <Next> and choose the option marked "Create a new certificate", and click <Next>. You can then choose to either prepare the certificate request and sent it later, or to send the certificate request immediately to an online CA. If you are using a third-party CA and are connected to the Internet choose the second option, otherwise choose the first option.

Enter the name for the certificate, typically this will contain the name of the organization, purpose of the certificate and any other pertinent information that will help you distinguish it.

You should choose a bit-length of at least 2048 bits, and leave the other options unchecked unless you are using the server outside of the United States, in which case you will need to choose the "Server Gated Cryptography (SGA)" option. Click the <Next> button when you are finished.

Now enter the organization and organizational unit name that best describes who is requesting the certificate. Click <Next> when you are finished.
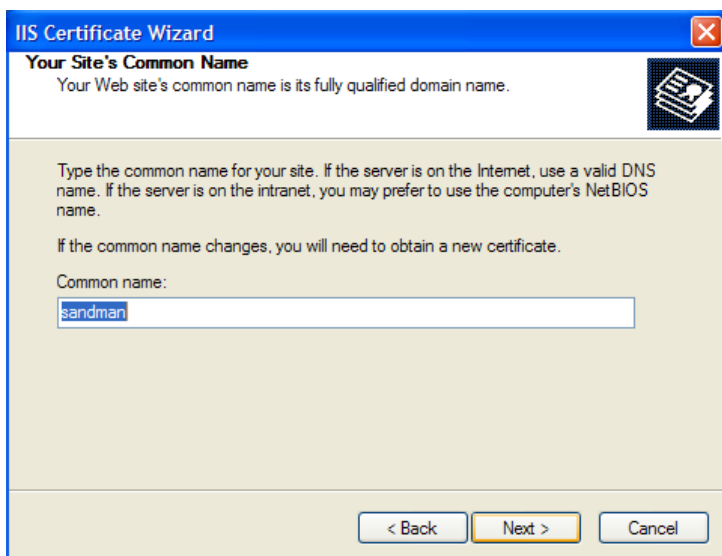
Next enter the "common name" for the web site that will be using the certificate. For a website that will be accessed across the Internet, this should the fully qualified domain name (e.g. www.mysite.com), whereas for a website that is limited to a local intranet, the computer name will suffice (e.g. myhost). Click <Next> when you are finished.
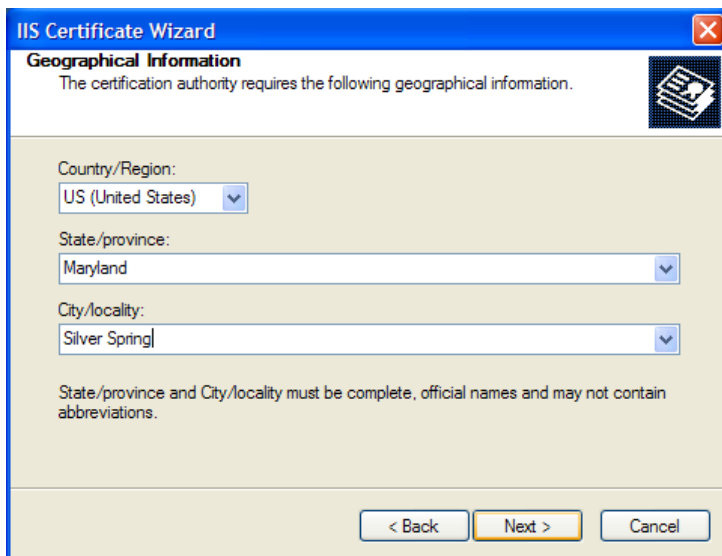
Next enter the country / region, state / province and city / locality that best describe where the web-server will operate or where the organizational entity resides. Once you are finished, click <Next>.
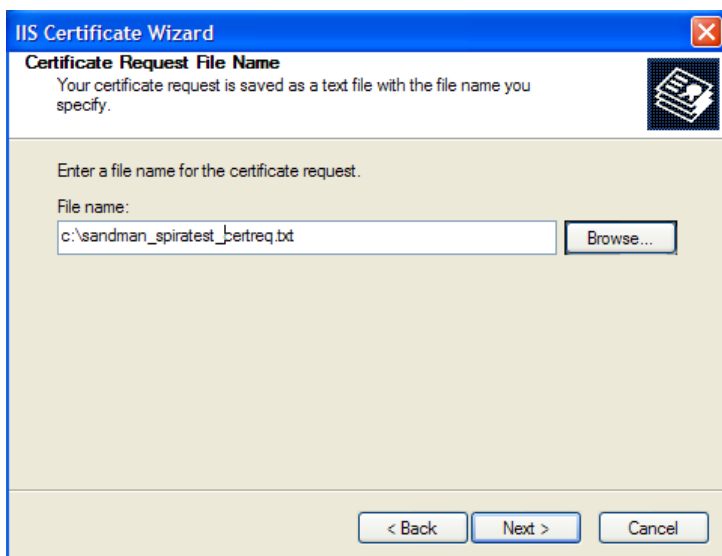
Next, enter the filename that you want to use for the *certificate request file*. This is the file that you will send to the Certificate Authority (CA) to request an SSL certificate. This filename should be memorable and describe what the certificate is for. The file extension should be `.txt`. Click <Next> once you have finished entering the filename.
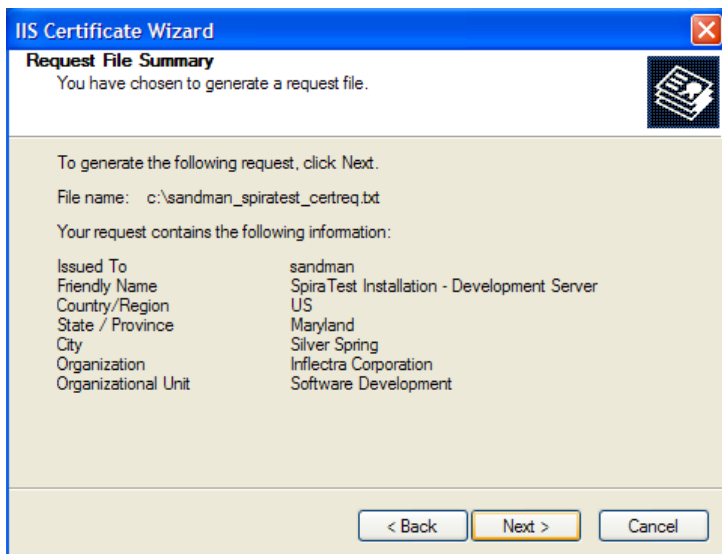
Finally, you will get a confirmation screen that verifies the information you have entered. If you want to make changes, click the <Back> button, otherwise click <Next> to actually generate the certificate. Once finished, you will now have the certificate request file that you can send to the Certificate Authority (CA) to process your request.

Once the CA has processed your request, they will send back the actual SSL certificate that you can install onto your web-sever. The next steps will describe how to install the certificate once you receive it back from the CA.

Once you have received the SSL certificate back from the CA, save the file onto your hard-disk with the file-extension `.cer`. Now open up the IIS management console (as described above), right-click on the "Default Web Site" icon and choose "Properties". Now select the "Directory Security" tab, and click the button marked <Server Certificate> under the heading "Secure Communications". When the dialog box appears, choose the second option – to process an existing request. This will bring up the following dialog box:
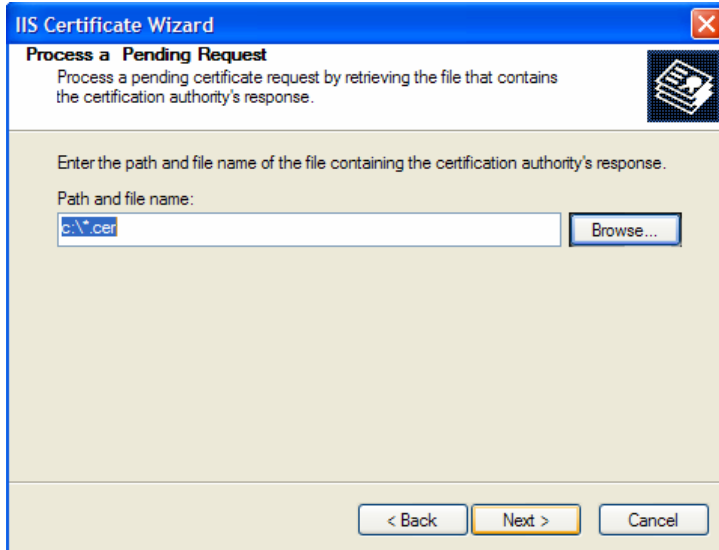
Now, browse to the place on your hard disk where you saved the SSL certificate (with extension .cer) and select the file you saved. Click <Next> to load the certificate. Once the certificate has been loaded, all that remains is to tell IIS to require a secure HTTPS connection, so that users don't attempt to access the website over the unencrypted HTTP protocol.

From the IIS properties dialog box, click the button marked <Edit> under the "Secure Communications" heading:
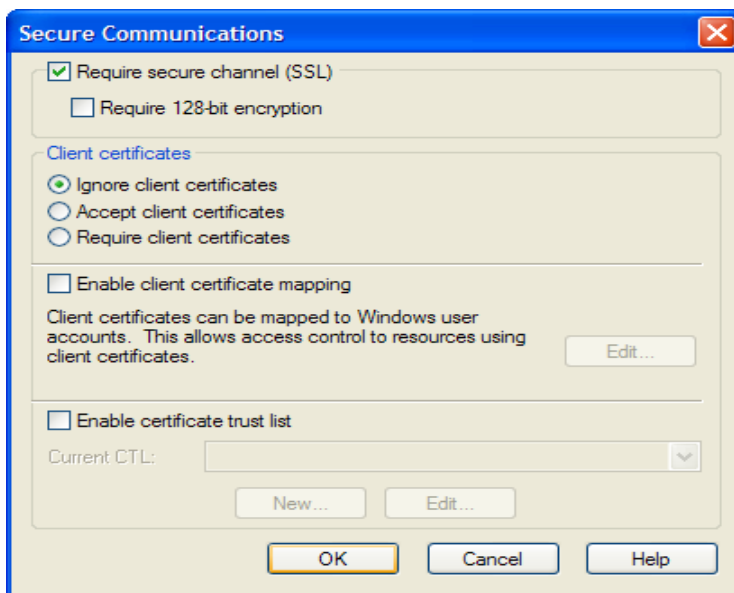
Check the box marked "Require secure channel (SSL)", and click the <OK> button. You have now successfully configured IIS for secure HTTPS data transmission.

4.3. Appendix C – Sending Email through IIS

This section outlines the steps that you need to take to configure your IIS web server to send email notifications from SpiraTeam®. Since email configurations can vary greatly between environments, please check with your local IT personnel for the correct settings that should be used. This section assumes that you have an SMTP mail-server available on your network that is capable of relaying the email from the IIS server.
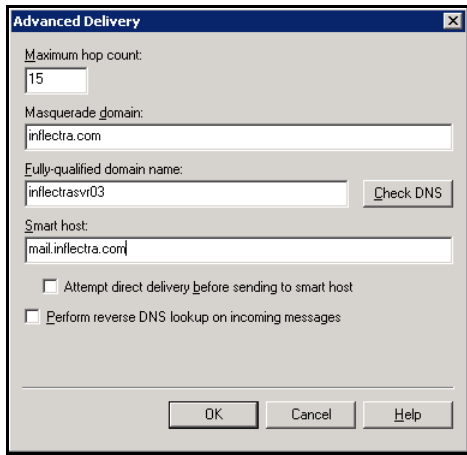
First open up the Internet Information Services (IIS) Manager on your server and expand the Default SMTP Virtual Server node:
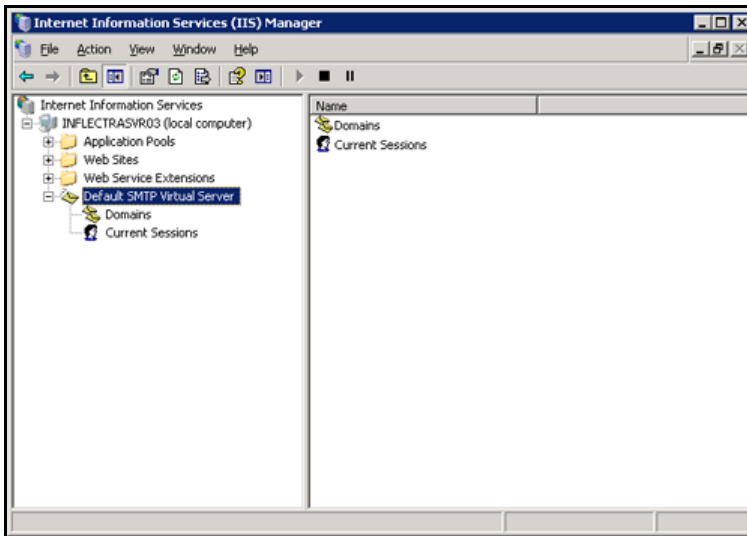
Right-click on the "Default SMTP Virtual Server" node and click on "Properties". Then select the "Delivery" tab on the dialog box that pops-up:
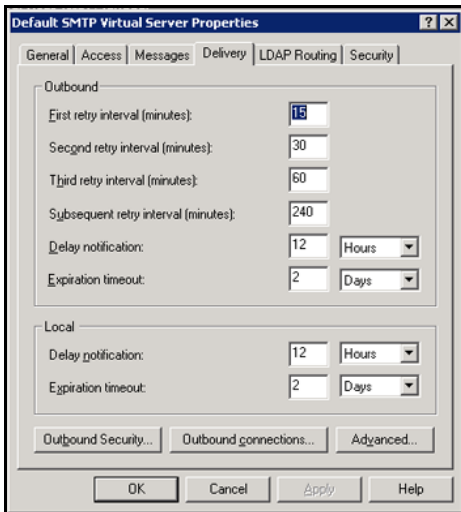
Now, click on the <Advanced> button to bring-up the advanced delivery configuration screen:

In this dialog box, you should enter the following information:

> **Masquerade domain:**
> This is the domain name that you want emails from SpiraTeam® to look like their being sent from. This is typically the domain name of your organization (e.g. mycompany.com)

> **Fully-qualified domain name:**
> This is the fully qualified domain name of the IIS server that SpiraTeam® is installed on (e.g. iisserver.mycompany.com).

> **Smart host:**
> This is the fully qualified domain name of the SMTP mail-server that will actually be used in delivering the emails. (e.g. mail.mycompany.com). You will need to get the name of this from your IT personnel.

Once you have updated the settings, click the various <OK> buttons and you should now see emails being delivered from SpiraTeam®. Note: the email address that is used as the 'from address' for all emails generated by SpiraTeam® is the email address stored in the Administrator user's profile. You should edit that user's account and make sure their email address is a valid email address in your environment.