Terms

This Windows SharePoint Services Operations Guide (WSSOPS) from the Computer Information Agency is provided as is. Every effort has been made by the author to ensure that information provided is correct however this cannot be guaranteed.

By using the Guide you also acknowledge that any work performed on production systems is a potentially dangerous act and may involve significant business risk and downtime. You hereby agree to release, waive and discharge the Computer Information Agency and/or the author from any liability incurred to yourself, your business or customers for any and all loss or damage, and any claims or demands therefore on account of problems arising from the use of this Guide.

By using this guide you hereby assume full responsibility for any risk to computer systems, now and forever arising out of, or related to the use of this Guide on any computer system.

Distribution and Duplication Guidelines

This document is copyright and only available directly from the Computer Information Agency. This work is now licensed under Creative Commons.

By using this Guide you agree to these terms.

Index

15.1 Scope

SharePoint Foundation Server 2010 (WSF) security relies on external security providers which are typically Windows Domains to control user access to the WSF server. Security can also be provided through an SQL database. By default, you will need to add network users to a WSF site and provide them with suitable rights. It is important to note that these rights can be independent of other network rights if desired.

This chapter will provide you with an understanding of the security mechanisms that are incorporated into WSF.

15.2 Security

Access to the SharePoint Central Administration web site is restricted to any user or group that is a member of the Local Administrators group on the WSF server. By default the network domain group, Domain Admins is always a member of the Local Administrators group and thus every network domain administrator has full access to the Central Administration web site.

Domain Admins by default do not have access to WSF data sites. However, if they can access the Central Administration web site then they can easily add themselves as Owners to any user site.

You can grant any user account from a network domain or a local server account, access to any WSF site. You can also do the same using security groups.

By default all WSF sites have these permission levels defined:

> *Limited Access* – this allows a user to access information in a specific list or document library but not the WSF site. What good is that you may ask? Don't forget that access to WSF content is not only via a web browser. It is also possible to access WSF content from products like Microsoft Office. Thus, you can use a Limited Access account to allow a user access to the data contained in any WSF site, without giving the ability to actually view the site.

> *Read* – a user with these rights can read, copy and print WSF content as well as create alerts. They can't however make changes.

> *Contribute* – a user with these rights has all the rights of a Read user but can also create, modify and delete WSF content. They can also make personal views of lists, libraries and web part pages.

Design – a user with these rights has all the rights of a Contribute user but can make changes to the global view of lists, libraries and web part pages. They are also bale to create new document libraries and lists.

Full Control – a user with these rights has full access to all content and security of the WSF site. They can also create sub-sites.

15.3   Default WSF Groups

Some of the default WSF groups are:

- *Visitor:* allows the user to open and read information, including documents, pictures and list contents. The user cannot however modify or delete information.
- *Member:* allows the user to do everything that a visitor can do as well as create, modify and delete information including news, documents, and contacts.
- *Owner:* has complete access to the site. Can add and delete other members and change their access. Think of a WSF site owner as a WSF administrator.

15.4   Adding users to WSF
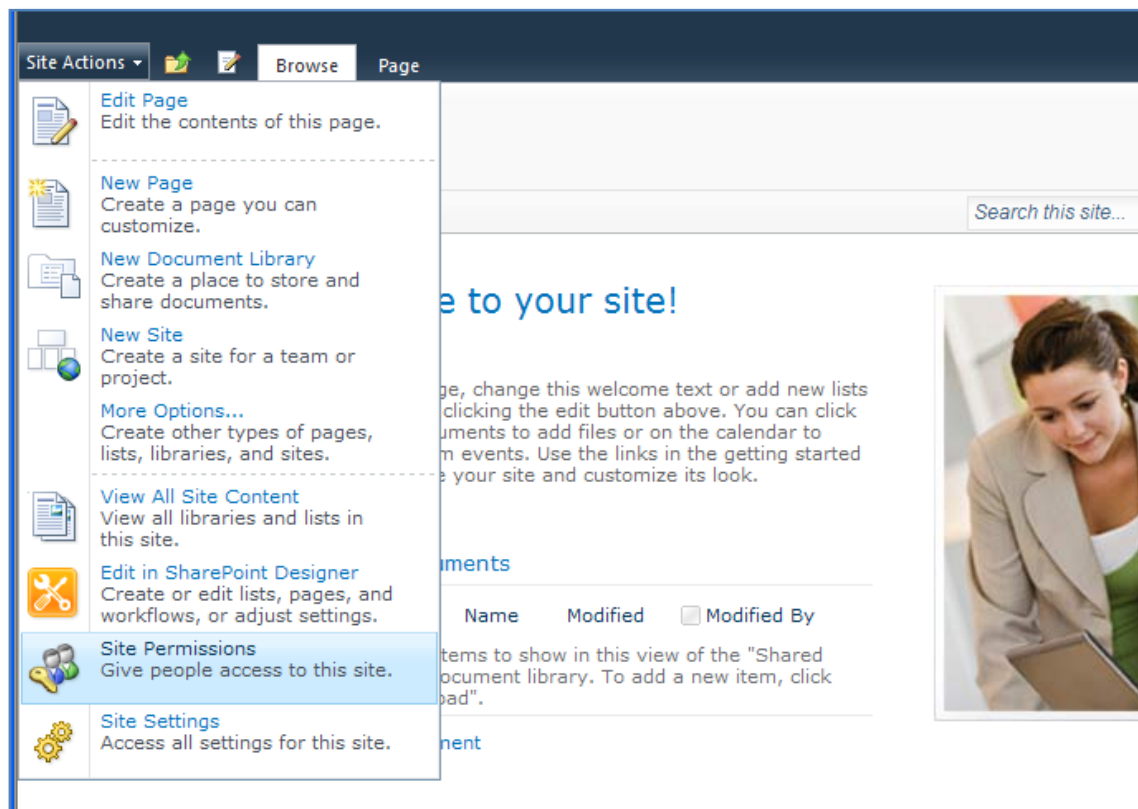
To add users to your WSF site logon to your site as an administrator and select the **Site Settings** from the upper left of the *Quick Launch* bar on the left. Then select **Site Permissions** from the menu that is displayed.
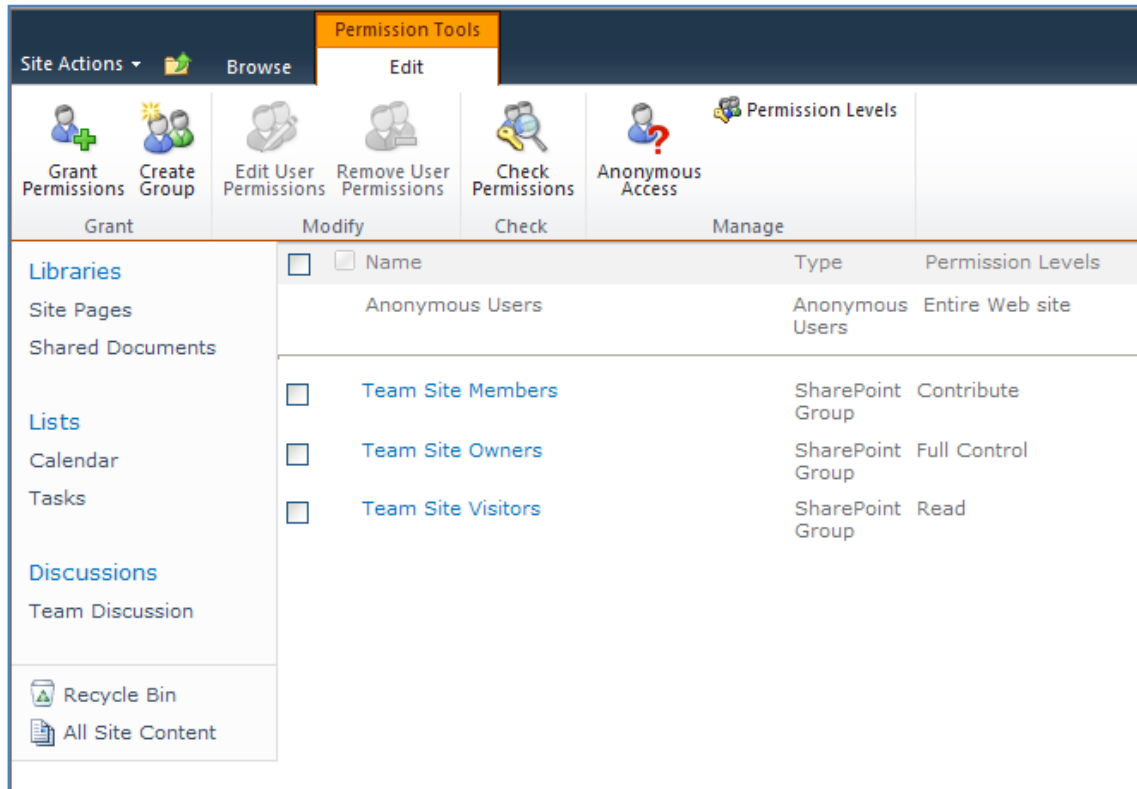
In the top middle of the window you will see a list of WSF groups (normally *Team Site Members*, *Team Site Visitors* and *Team Site Owners*). Click on any of these groups to display their members. In the case above we have selected *Team Site Members*.
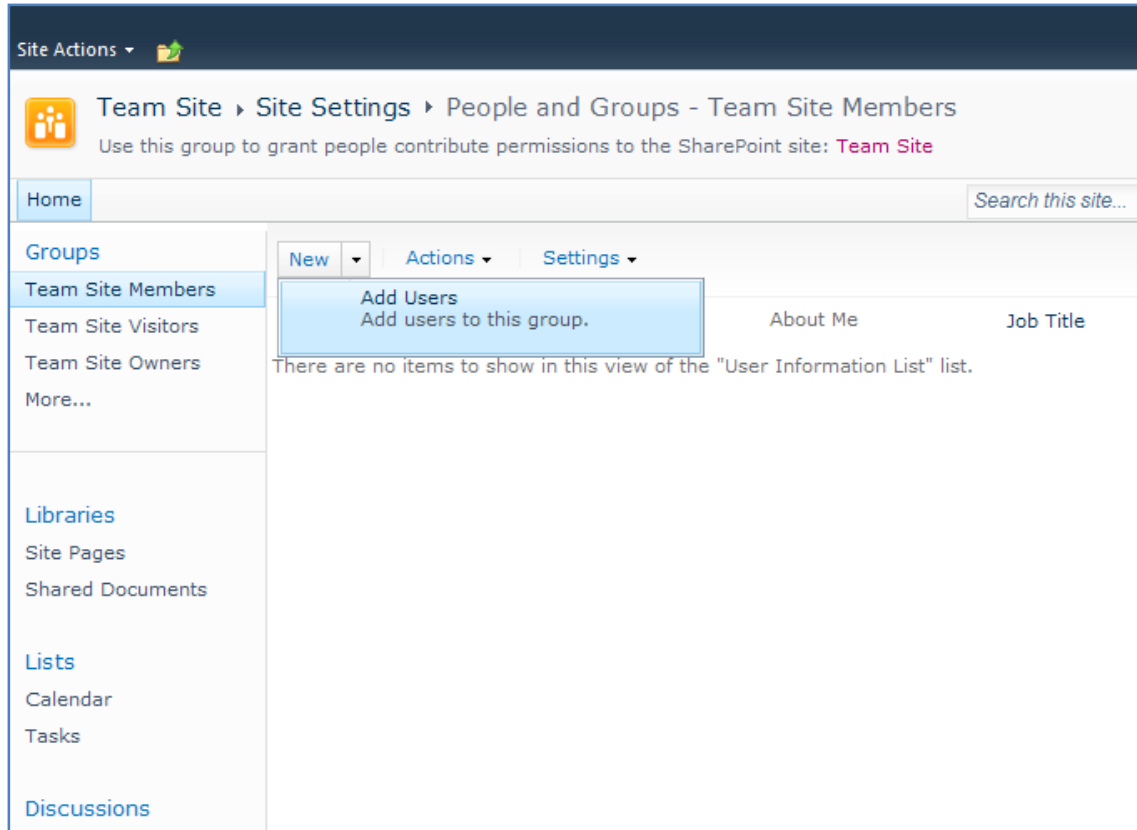
To add users select **New** | **Add Users** from the menu across.
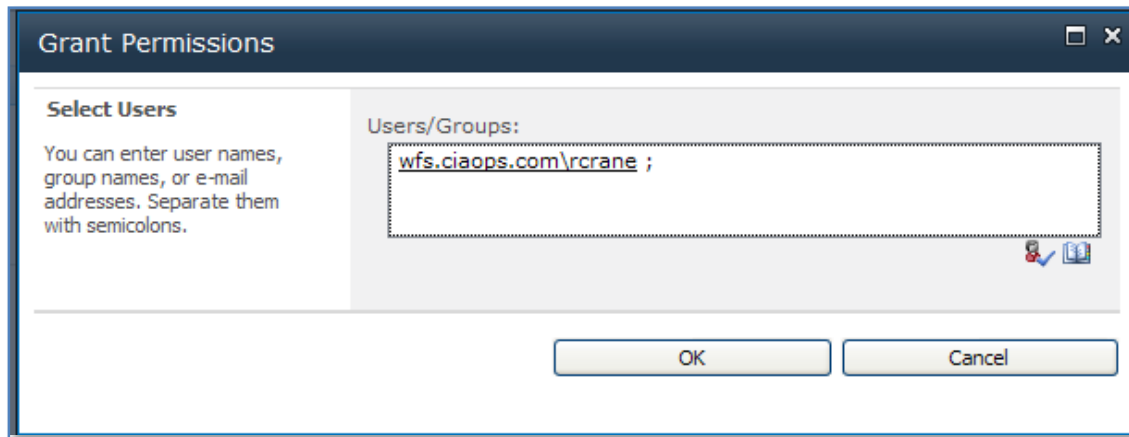
You should now see the above screen. Into the area under *Select Users* you can enter the name of network users or groups. You can enter new users simply by typing their name or network logon. In some cases you may need to use domain/login name. To ensure that WSF can add the specified user press the *Check Names* icon in the lower right of this box (i.e. the one with the little check next to it).

When you press *Check Names* WSF will check that the user details you entered are correct. If so it will place an underline below the name.
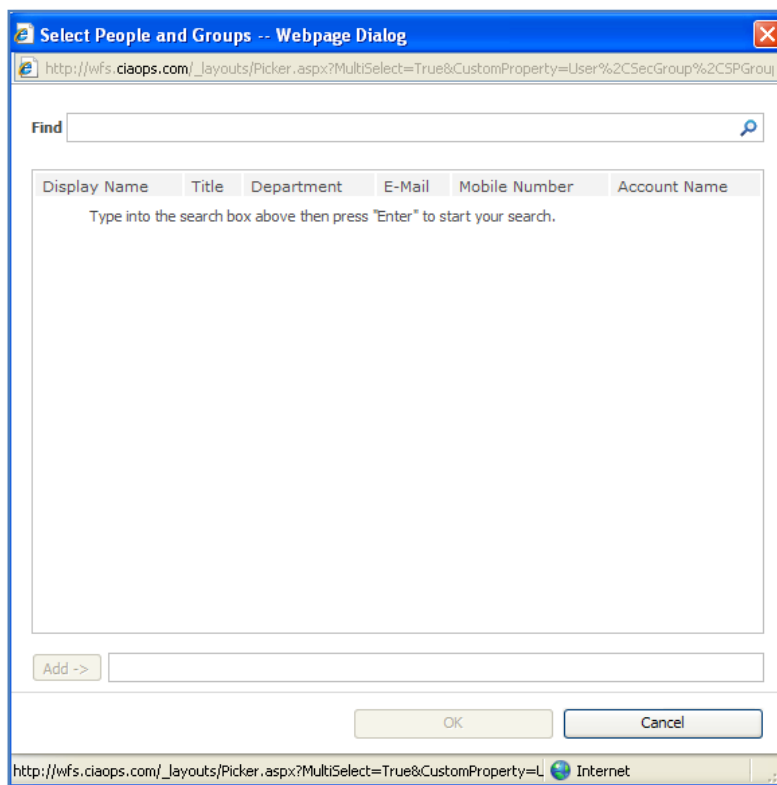
If you are unsure of the user details you can press the *Select People* icon, which is also in the lower right of this box (and appears like an open book). When pressed, you will see a window like that shown above. Simply enter the details of the user and press the **Find** button.

If that user can be located on the network then it will be displayed in the lower part of the window. Simply select the user and press that **Add** button at the bottom of the screen so the name appears next to the *Add* button. Press **OK** when you have completed finding all the users.

The users you added should now appear under the respective groups you allocated. To view and edit the details of a user simply click on their name or photo (if it exists).

Once you click on the user you are able to go in and edit their details by selecting **Edit Item** from the menu.
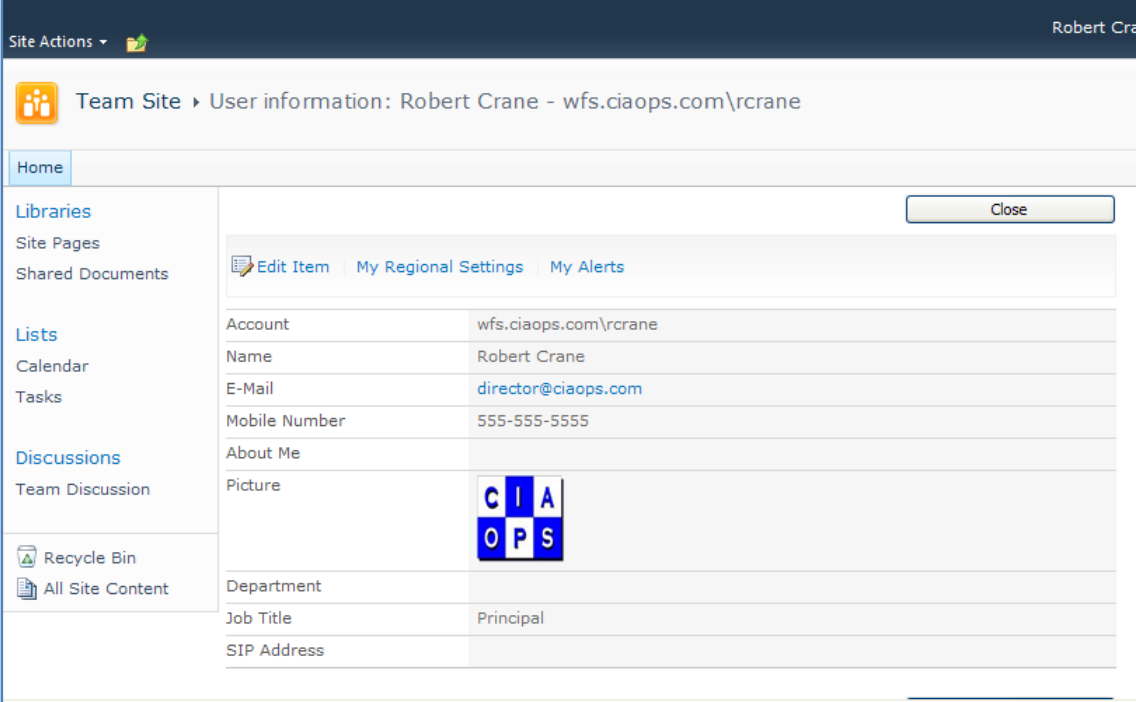
Once you have completed editing the information press **OK** to save and continue.

15.7   Enabling anonymous site access

Any anonymous access to WSF needs to be considered carefully. This is especially true if the site is exposed on the Internet. With anonymous access enabled unauthenticated users will be able to access the site. This access can be controlled via low level WSF permissions but initially the site must be enabled for anonymous access (since it isn't by default).
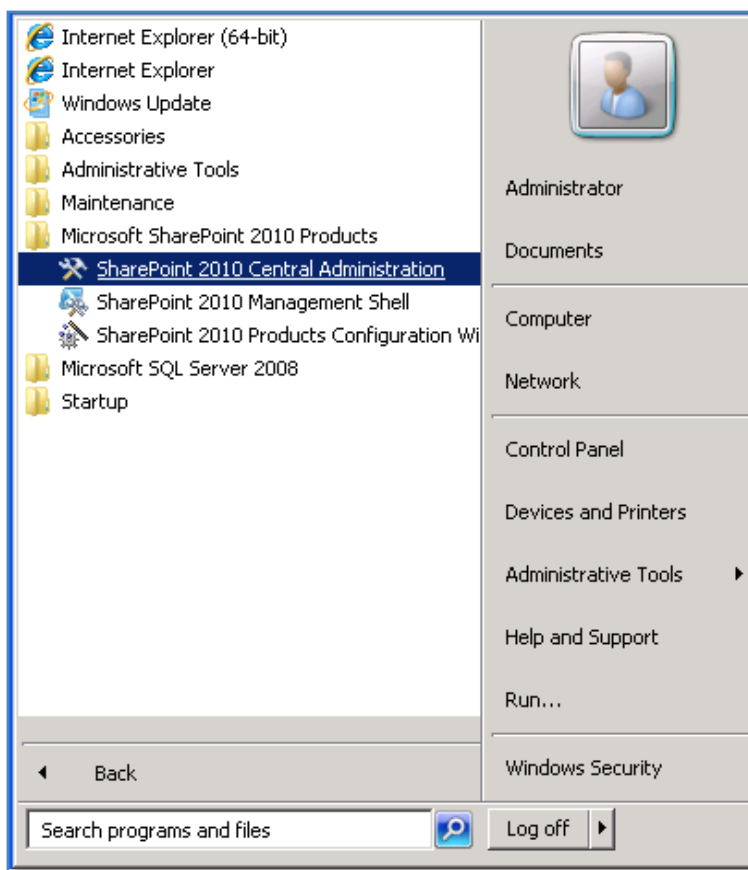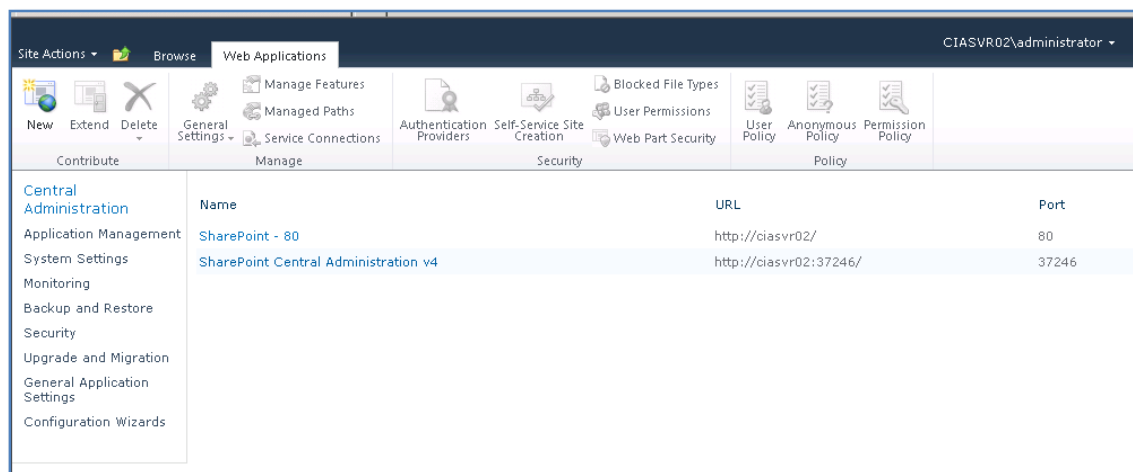
The first step is to run the SharePoint 2010 Central Administration by logging onto the
WSF server and selecting **Start | All Programs | Microsoft SharePoint 2010 Products |
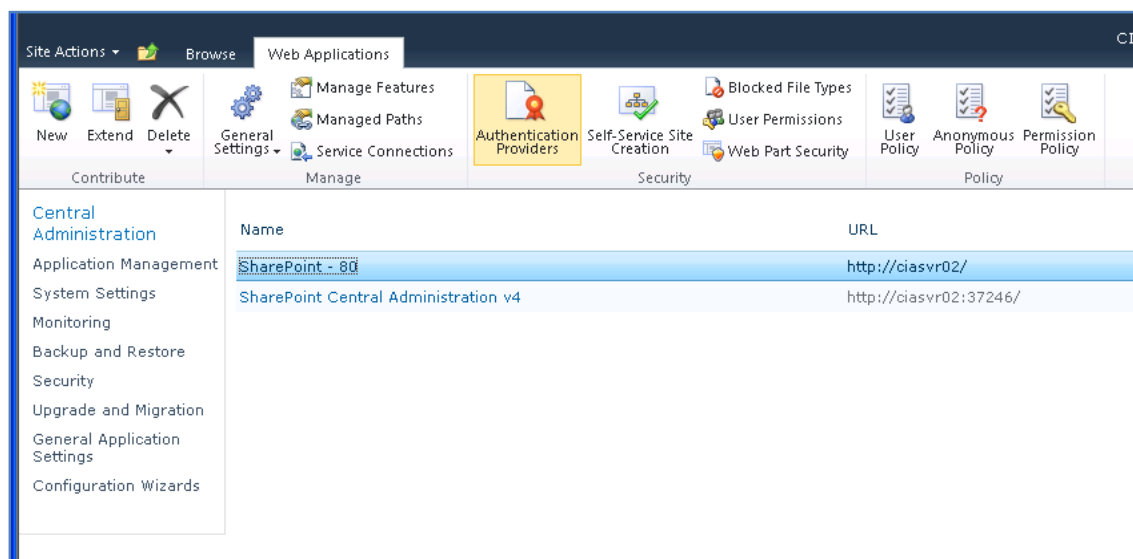SharePoint 2010 Central Administration**.
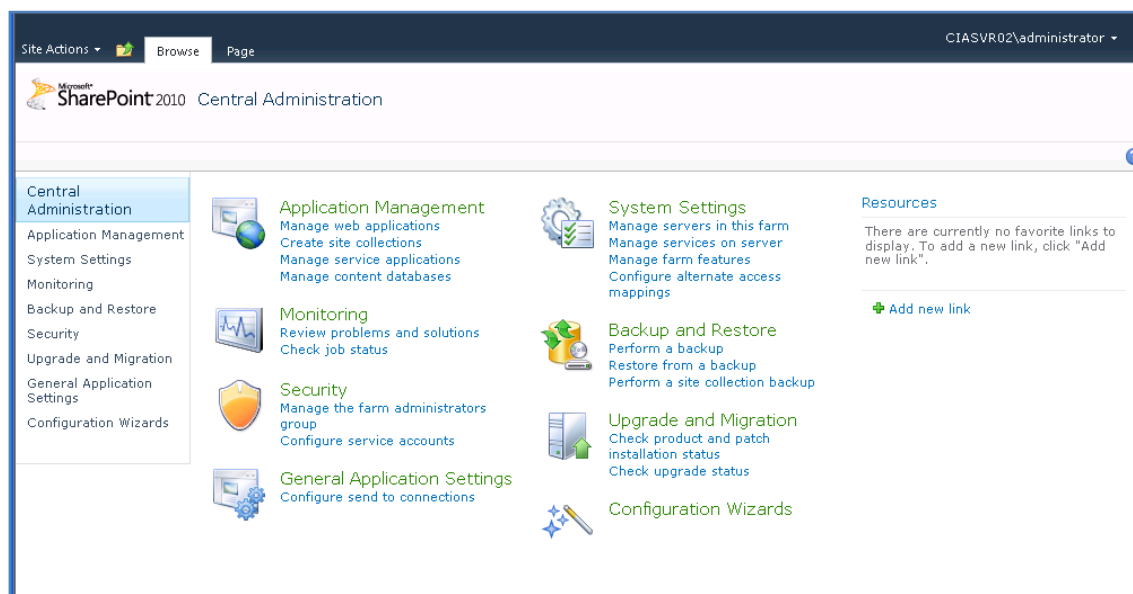
At the Central Administration site select **Manage Web Application** from under the *Application Management* section in the top left of the screen.
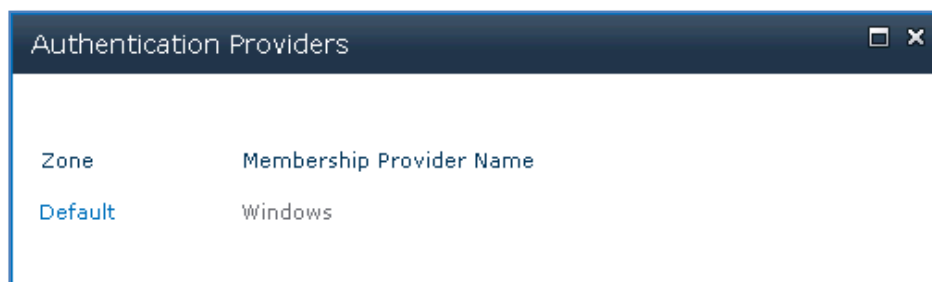

You should then see a list of SharePoint sites, including the Central Administration site.


Select the site that you wish to enable anonymous access for (in this case SharePoint – 80) by clicking on the entry.

When you do that button on the ribbon menu will be enabled. Click on the item **Authentication Providers** in the middle of the screen.

You will now see a window with all the authentication providers for that site. In most cases these providers will be Windows, although it is possible to have others.

Click on the hyperlinked Zone to select the zone for which you wish to provide anonymous access (in this case *Default*).
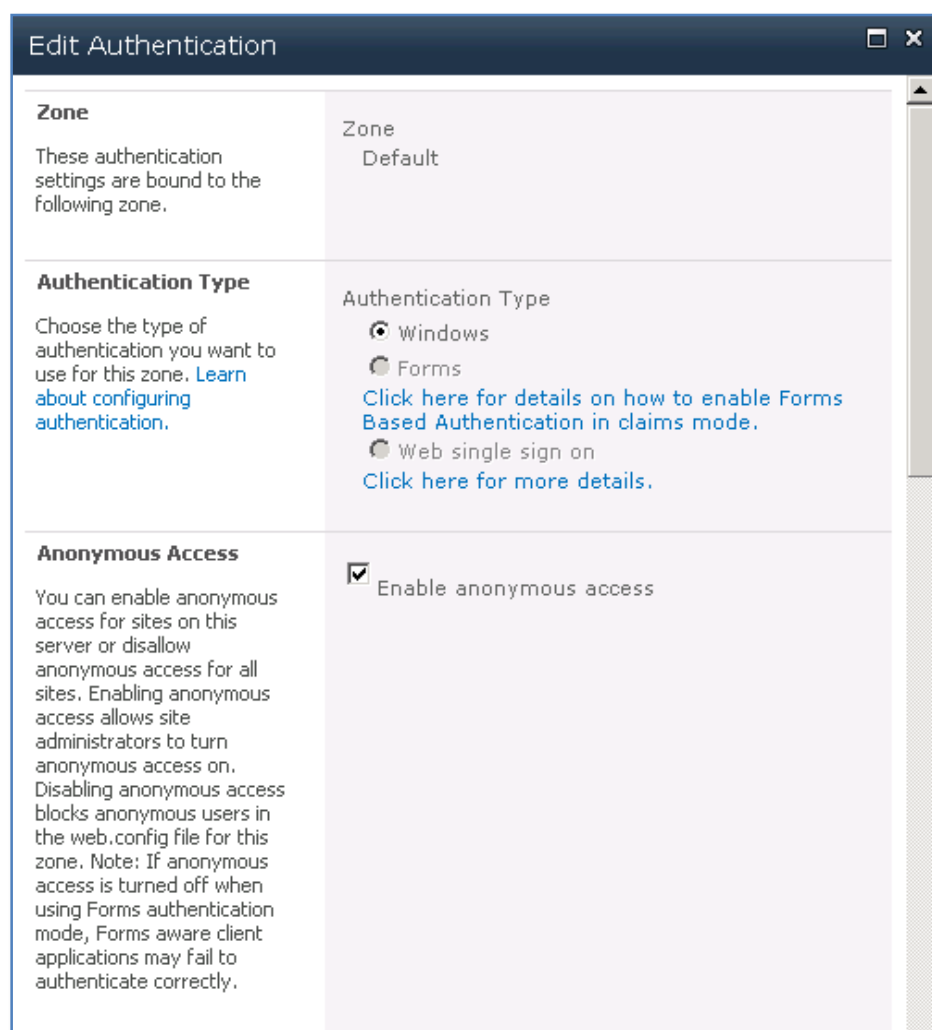
In the window that is now displayed you should find a section called *Anonymous Access* towards the middle. Simply place a check in the option Enable anonymous access and press the **OK** button to save the configuration.

Since WSF is a web application that uses Internet Information Services on the host Windows Server where you are running WSF anonymous access also needs to be granted here. By going through the above process the necessary steps have been completed by WSF. To check this, log in to the WSF server as an administrator and select **Start** | **Administrative Tools** | **Internet Information Services Manager**.
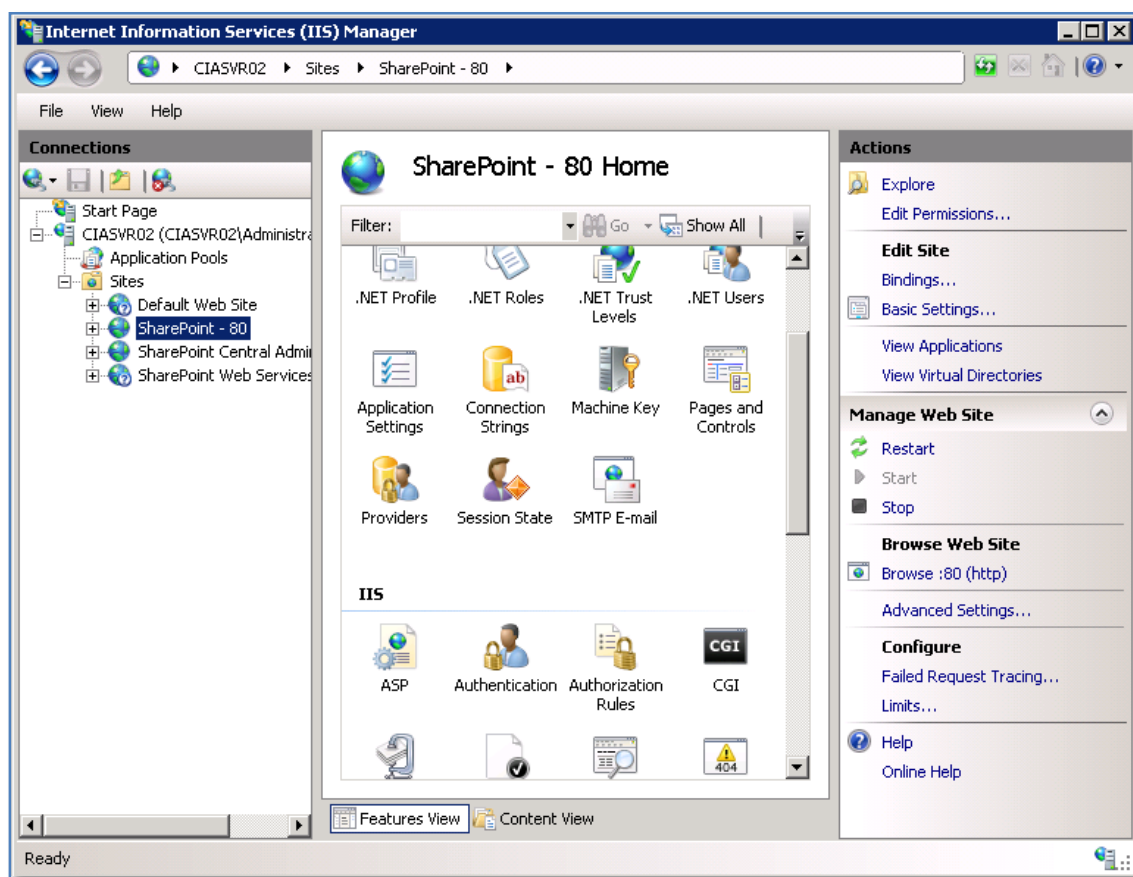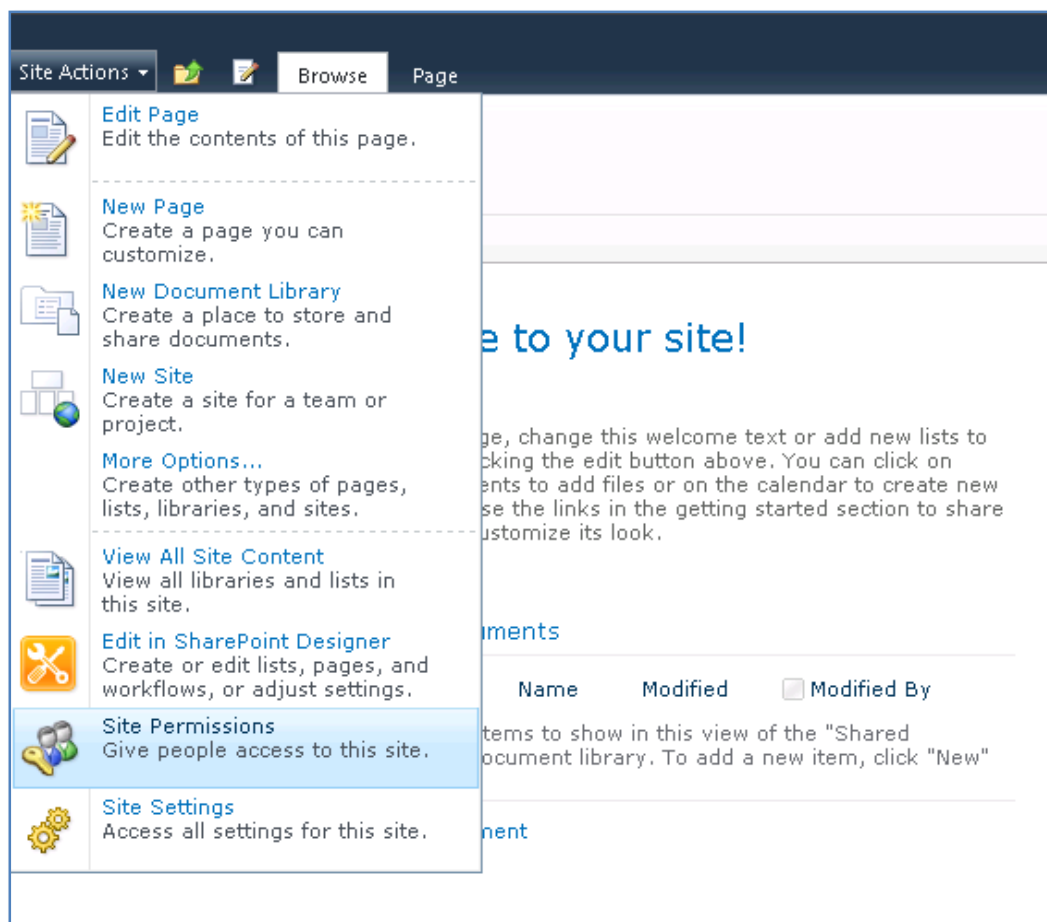

Locate the WSF site under the *Sites* folder (here it is called *Sharepoint – 80*). **Select it** and then select **Authentication** in the IIS section.
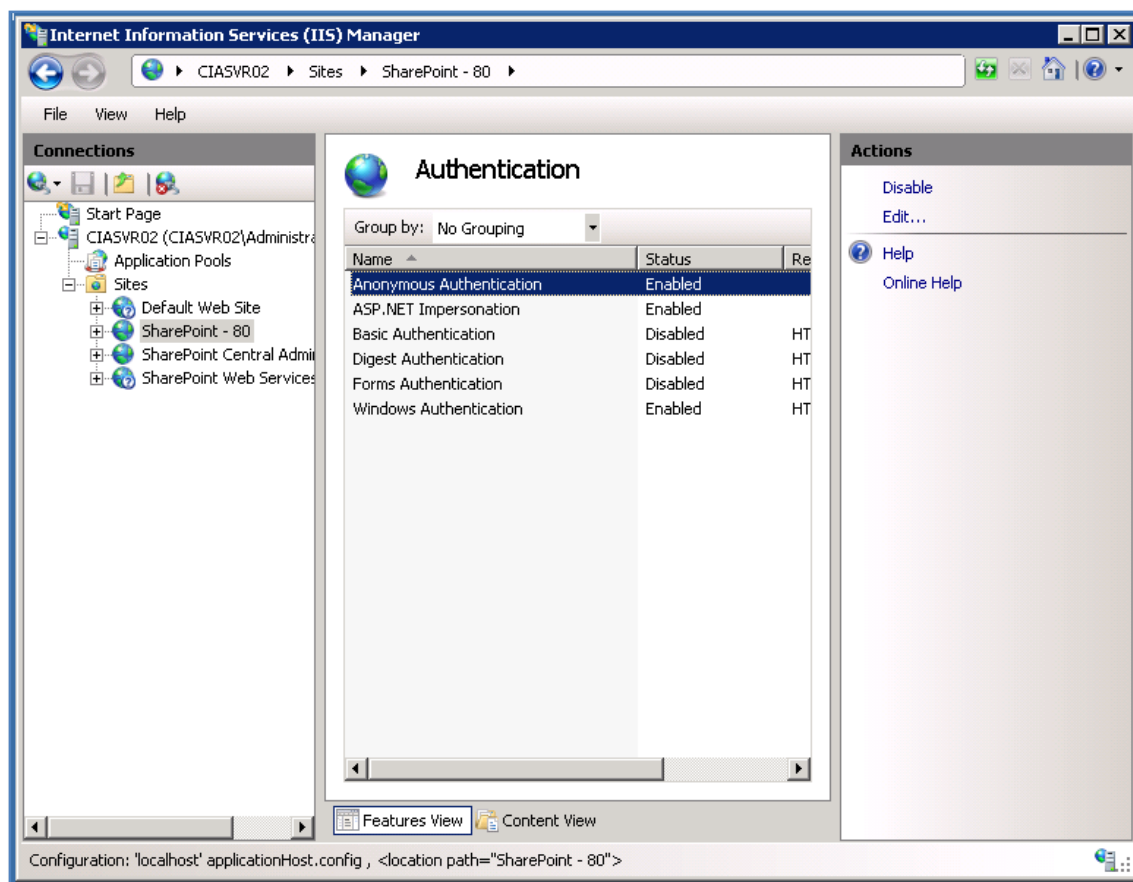
You will see that Anonymous Authentication at the top of the middle window is *Enabled*.

You now need to enable anonymous access specifically within the WSF site as well. Browse to the WSF site you wish to enable anonymous access with at least WSF site owner rights.

Click on the **Site Actions** area in the top left of the screen to display a pull down menu. Select the option **Site Permissions** from the list that appears.
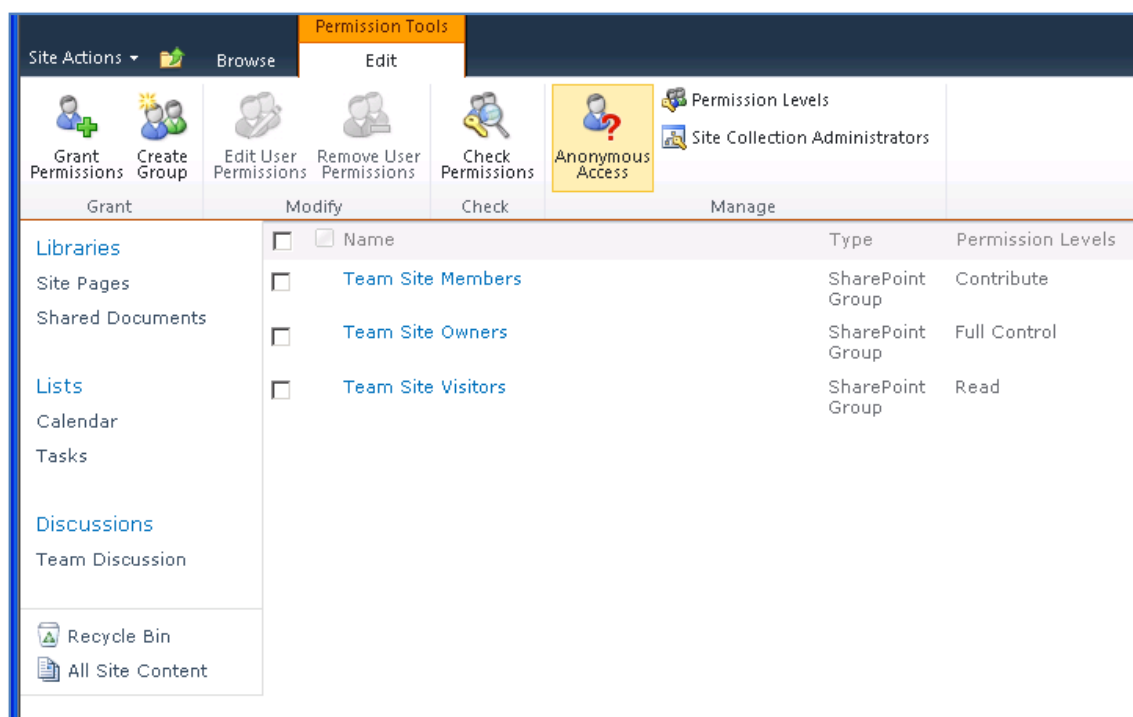
In the ribbon bar across the top select **Anonymous Access**.
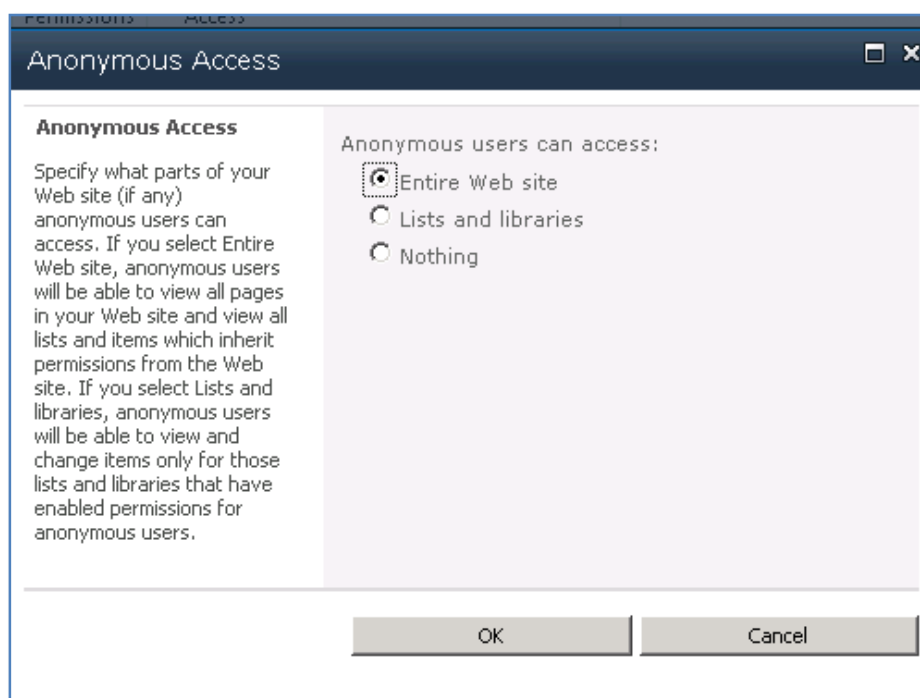
Select what level of anonymous access you wish to enable. The options are:

Entire Web site: any user can access any part of the WSF site including any sub-sites that inherit their permissions from this parent site.

Lists and libraries: any user can access any list or library in any part of the WSS v3 site that has been explicitly enabled for anonymous access. They are unable to navigate by viewing other pages and can only access the list or library via a direct link.

Nothing: unauthenticated users have no access.

In the window that appears select the option **Entire Web site** and press the **OK** button to save the configuration.
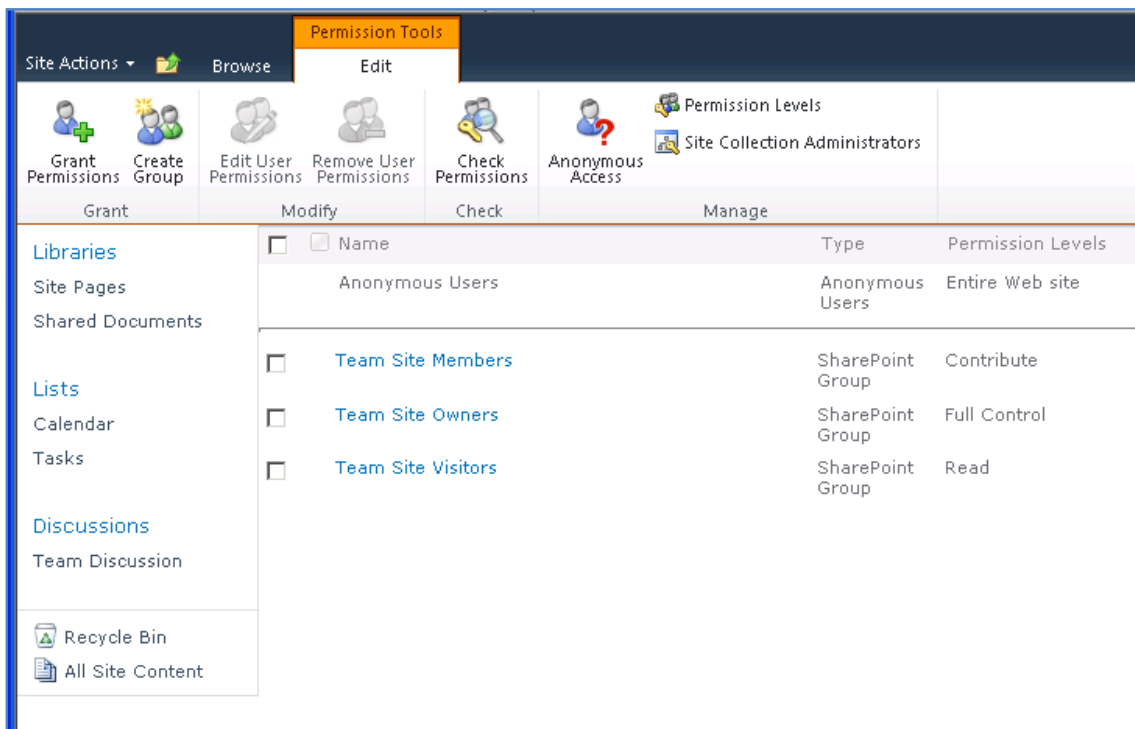

When you are returned to the site permissions area you will see an area called *Anonymous Users* above the other site users including the *Permission Level* they have been granted.
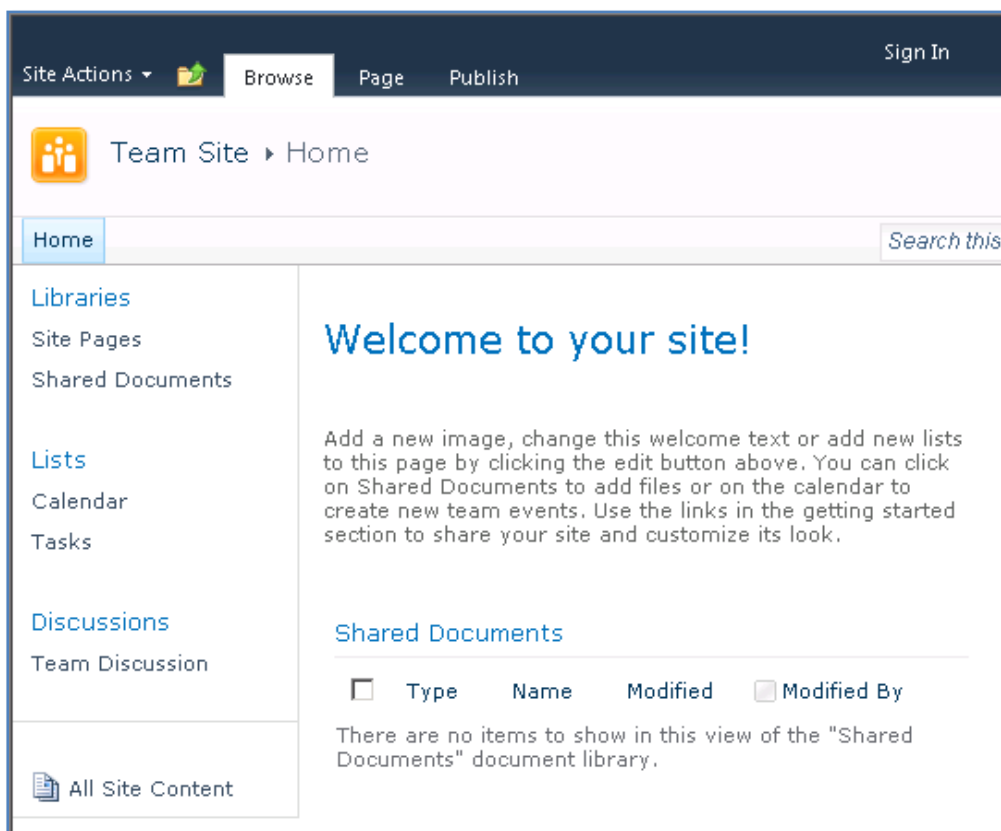
If you now open a new browser window and access your WSF site you should find that it is displayed as normal. However, in the top right of the screen you will see that instead of being logged in as a network user you are not logged in (denoted by *Sign In*).

If you click the **Sign In** link you will automatically be logged into WSF as the current network user.
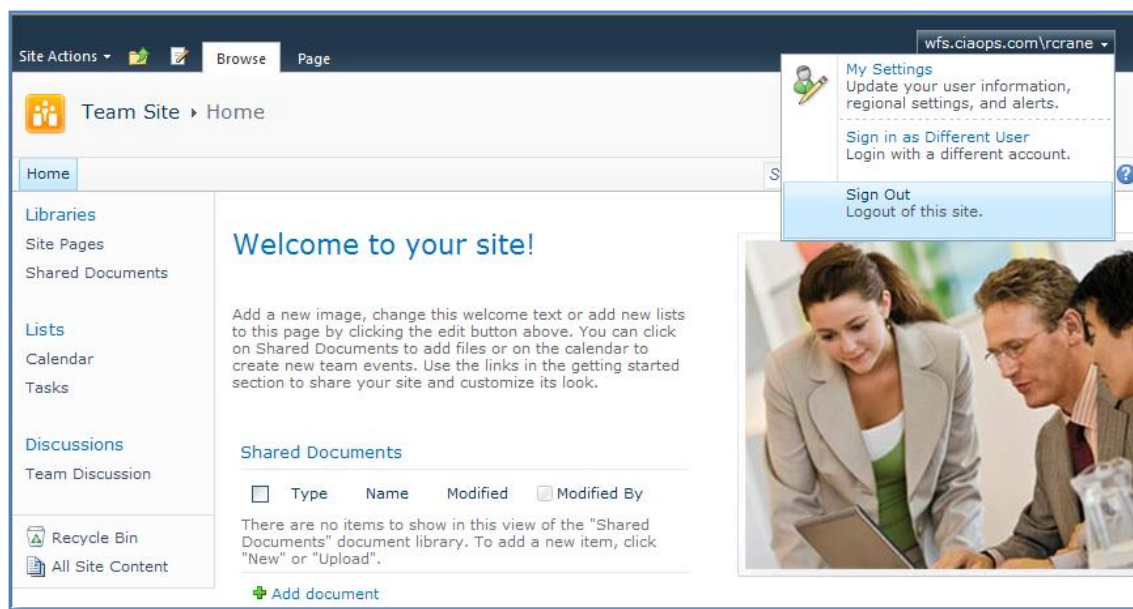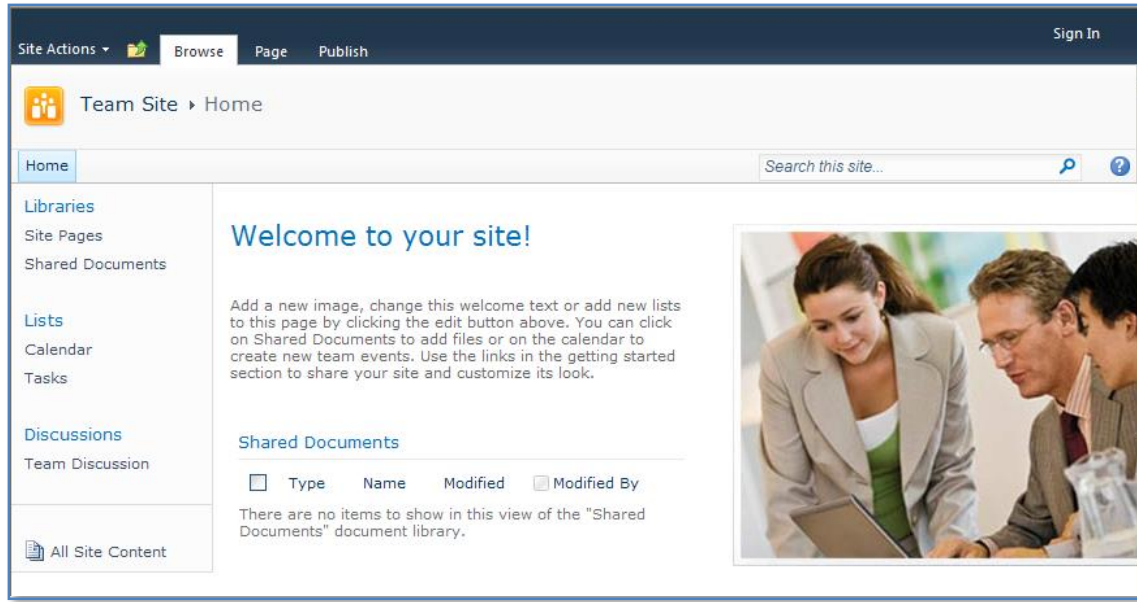
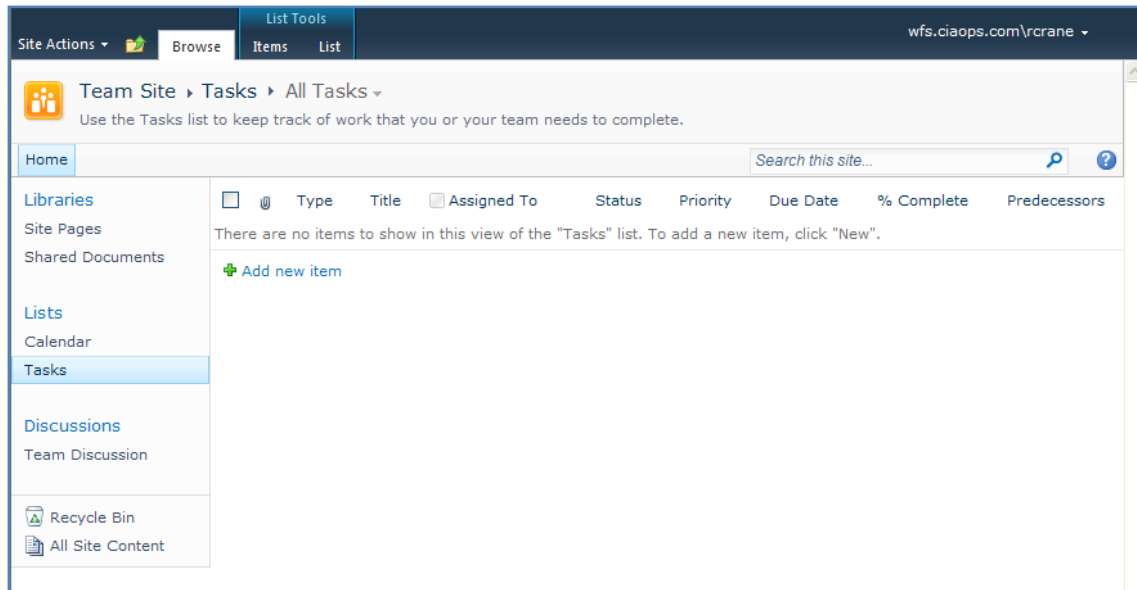If you pull down the arrow to right next to the login name you are able to select the option from a menu to **Sign Out**.
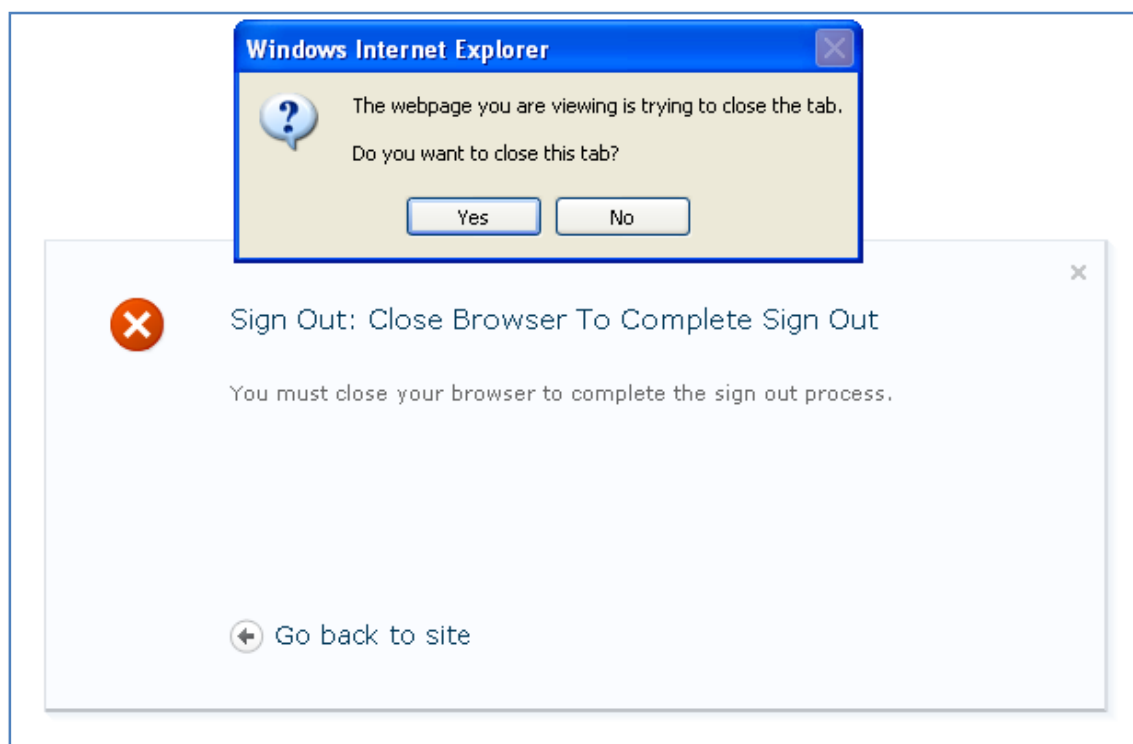
You will be signed out of the site. If you return to the WSF site again in your browser you will see that you are no longer logged in.

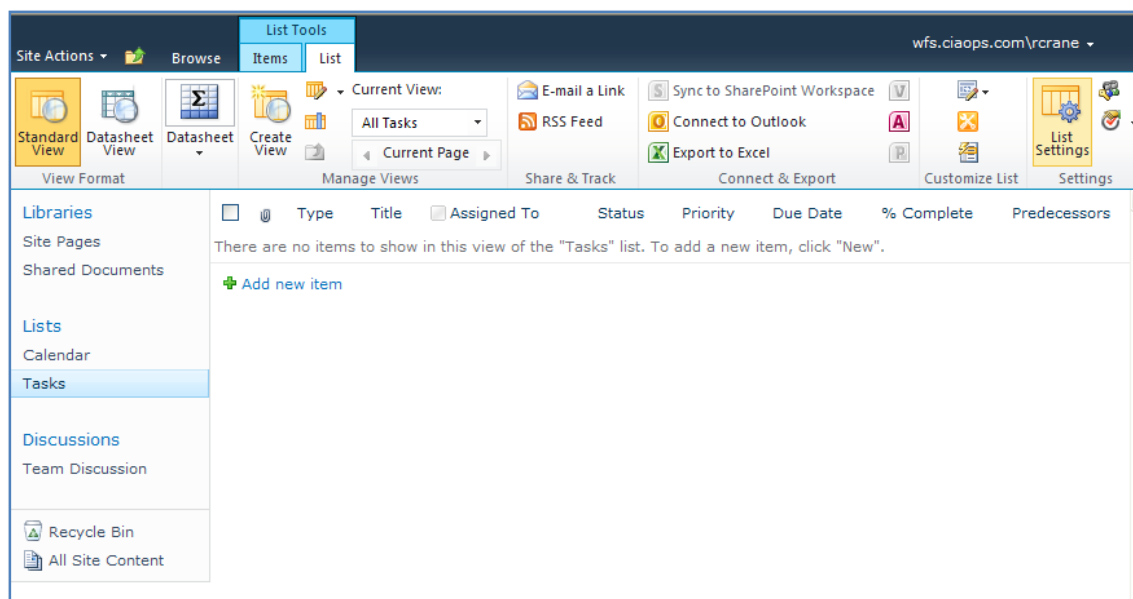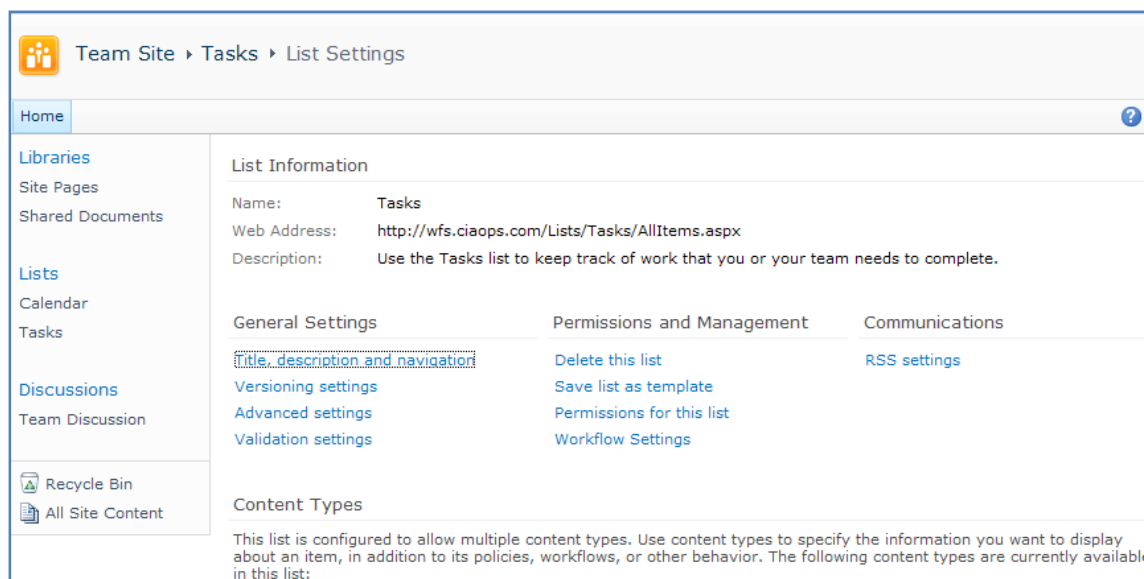You must again select *Sign in* the top right of the window to log in as a network user to this WSF site.

Finally, you need to allow anonymous access to the items in WSF. To do this, for example on an existing list, go to the list and select **List** under *List Tools* from the menu bar.
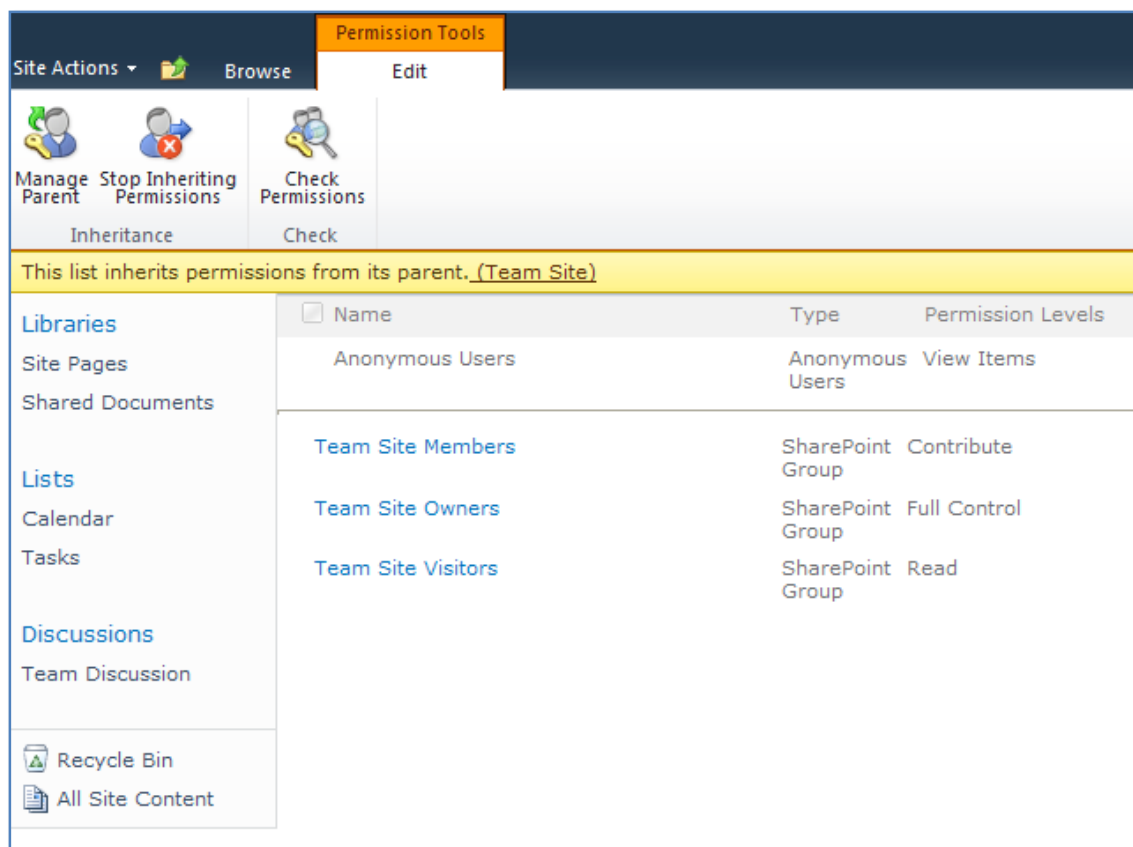
Then select list settings from the ribbon bar at the top right of the window.

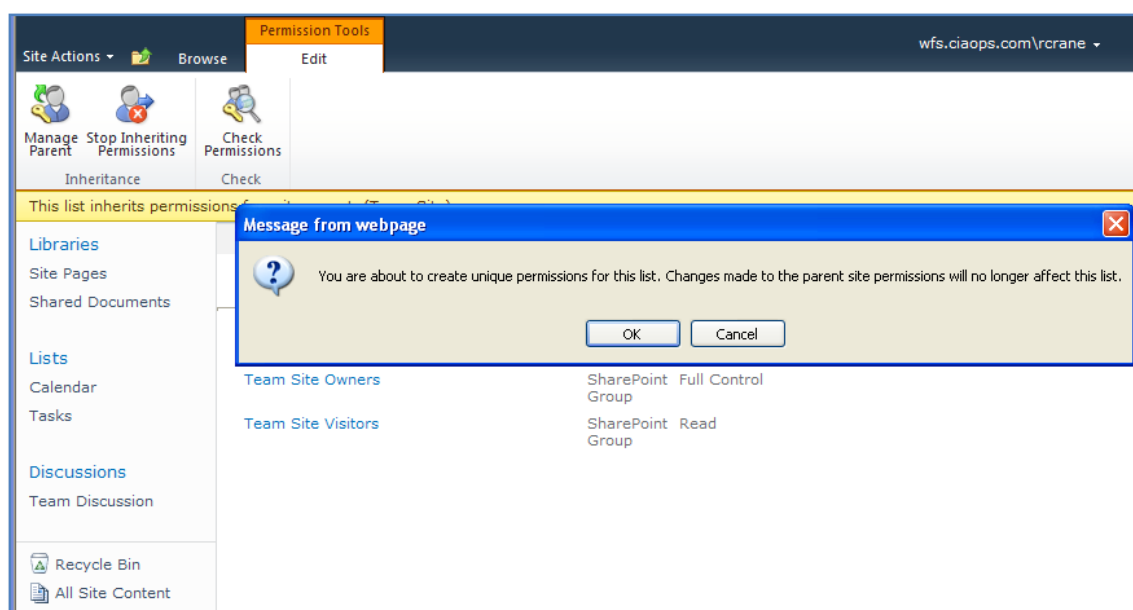In the list settings select **Permissions for this list** from *Permissions and Management* section.
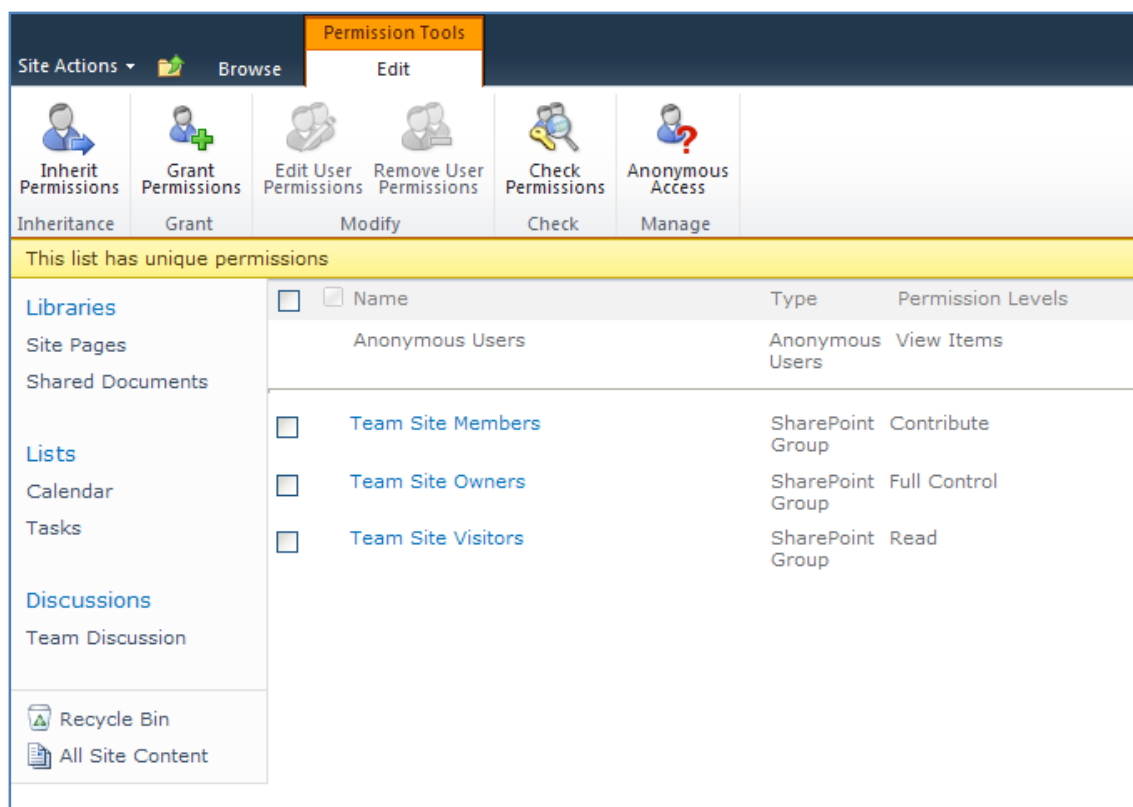
By default, the list will normally inherit its permissions from the parent site. To prevent this select **Stop Inheriting Permission** from the ribbon bar.


Press the **OK** button to accept the changes and continue.

You will be returned to the Permissions window. You will notice that menu bar now contains a number of additional options. You will also notice that Anonymous users have been already been added (due to previous inheritance) to the permissions and granted the ability to view items. To change this access select **Anonymous Access** from the ribbon bar.
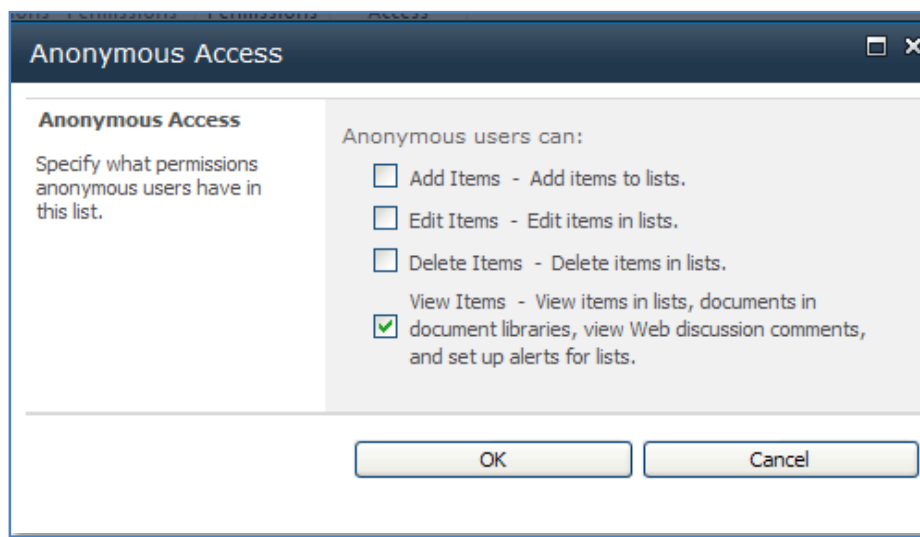
Set the permissions for anonymous users on this list and press **OK** to continue.

Any items already in the list will now inherit their permissions from the options that you have now set (including anonymous access).

15.9   Conclusion

This guide continues to be a work in progress and I encourage comments and feedback of any type. The only way that the Guide will improve if these is continued feedback.

Please send your comments and feedback to director@ciaops.com.