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.

http://creativecommons.org/licenses/by-nc-sa/4.0/

By using this Guide you agree to these terms.

Index

15.1   Scope

Windows SharePoint Services v3 (WSS v3) security relies on external security providers which are typically Windows Domains to control user access to the WSS v3 server. Security can also be provided through an SQL database. By default, you will need to add network users to a WSS v3 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 WSS v3.

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 WSS v3 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 WSS v3 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 WSS v3 site. You can also do the same using security groups.

By default all WSS 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 WSS v3 site. What good is that you may ask? Don't forget that access to WSS v3 content is not only via a web browser. It is also possible to access WSS v3 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 WSS v3 site, without giving the ability to actually view the site.
>
> *Read* – a user with these rights can read, copy and print WSS v3 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 WSS v3 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 WSS v3 site. They can also create sub-sites.

15.3   Default WSS v3 Groups

Some of the default WSS v3 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 WSS v3 site over as a WSS v3 administrator.

15.4   Adding users to WSS v3
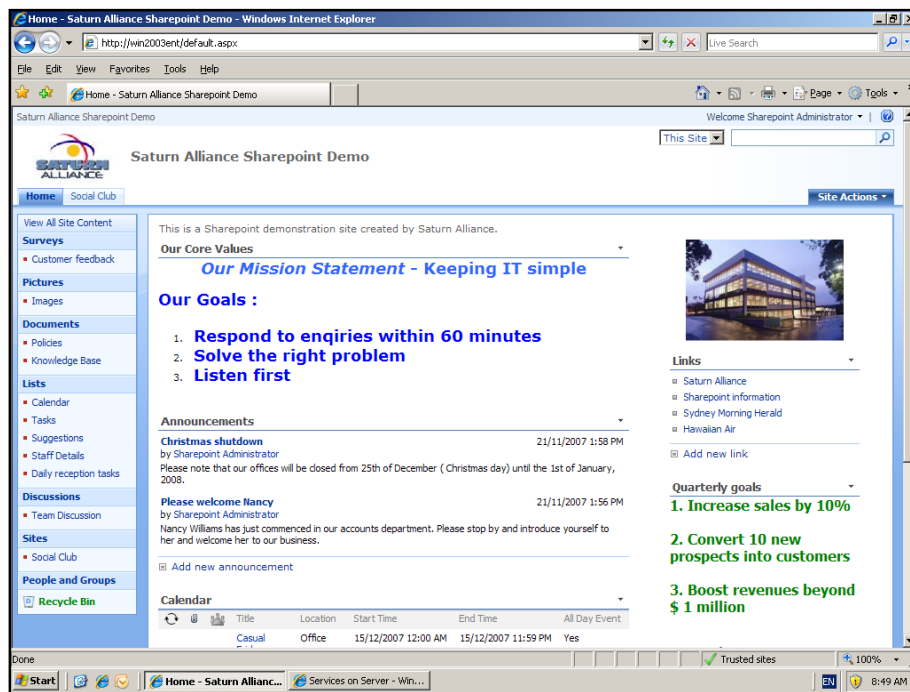
To add users to your WSS v3 site logon to your site as an administrator and select the **People and Groups** from the lower left of the *Quick Launch* bar on the left.
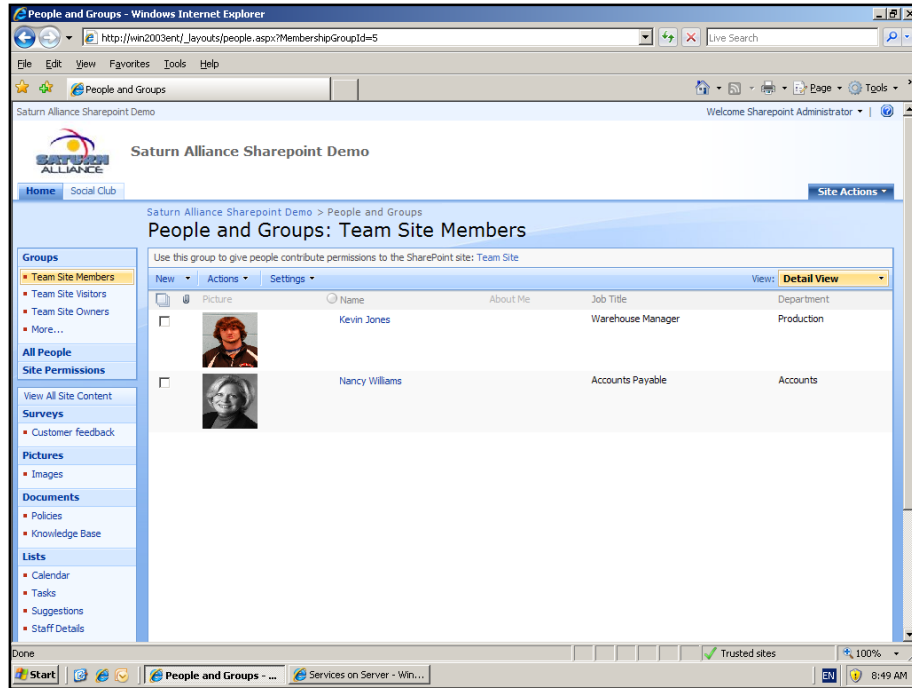
In the top right of the *Quick Launch* bar you will see a list of WSS v3 groups (normally *Team Site Members*, *Team Site Visitors* and *Team Site Owners*). Click on any of these groups to display their members. In the case above we have selected *Team Site Members*.
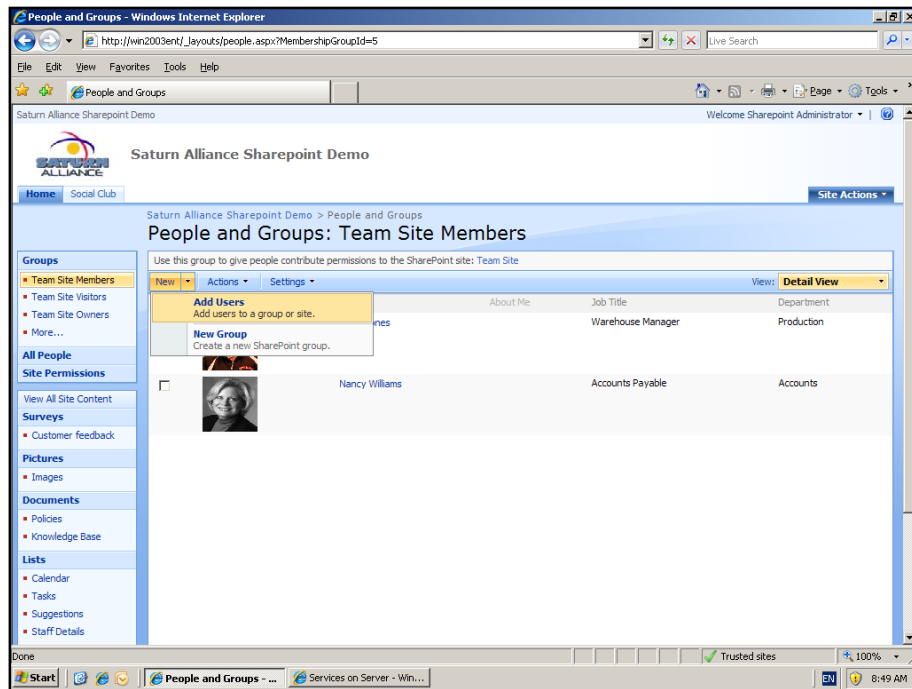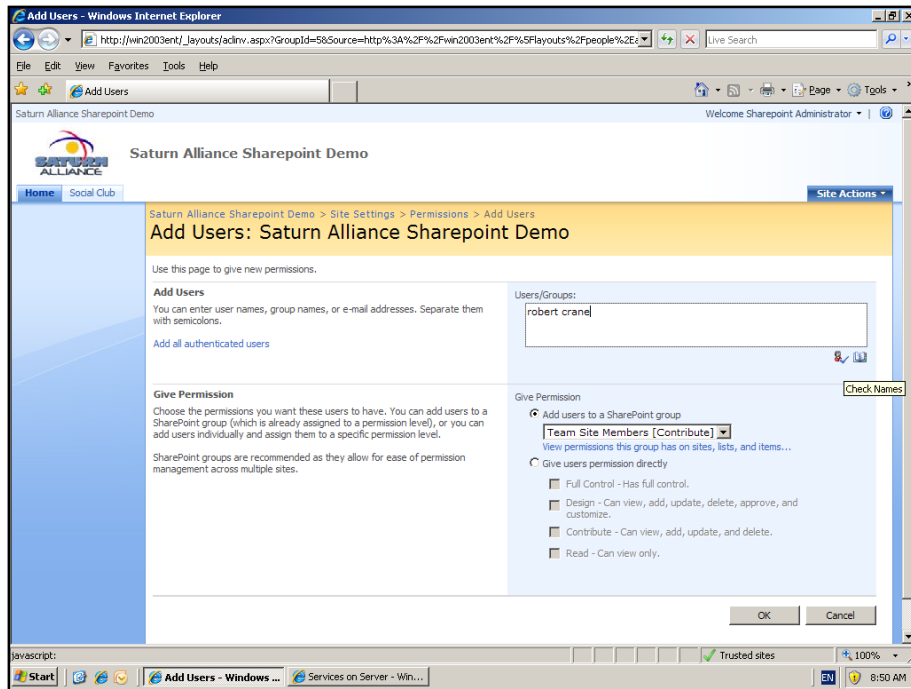

To add users select **New** | **Add Users** from the menu across.
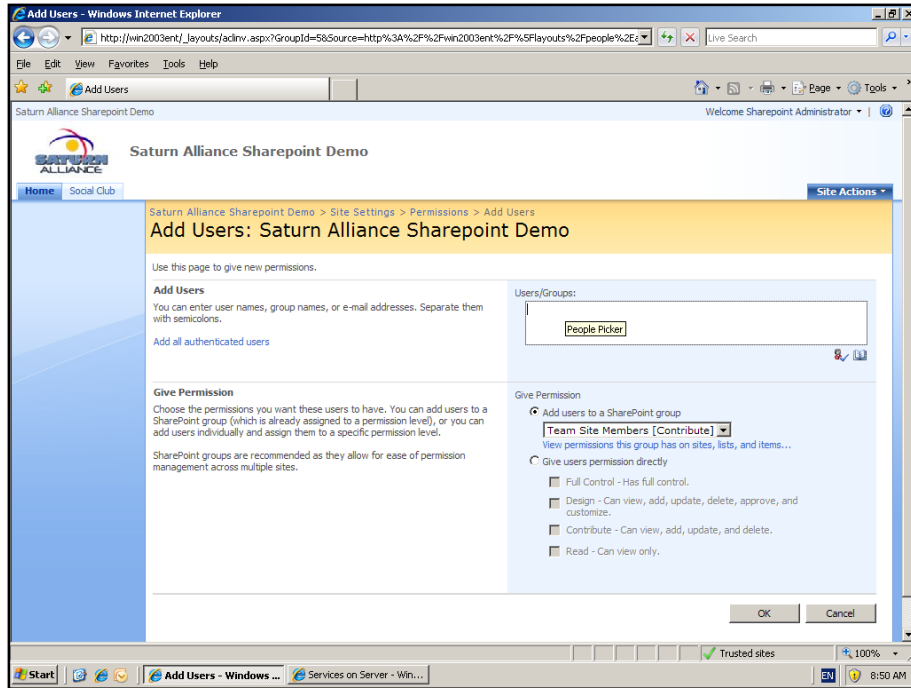
You should now see the above screen. Into the top area under *Users/Groups* you can enter the name of network users or groups. The lower section allows you to define what permissions these users have.

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 WSS v3 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).
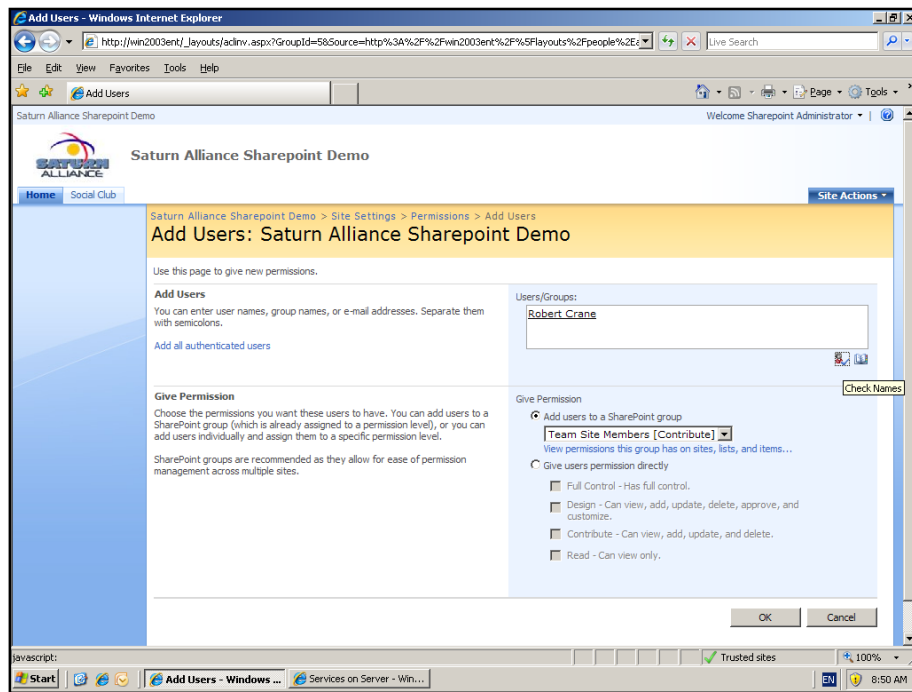
When you press *Check Names* WSS v3 will check that the user details you entered are correct. If so it will place an underline below the name.
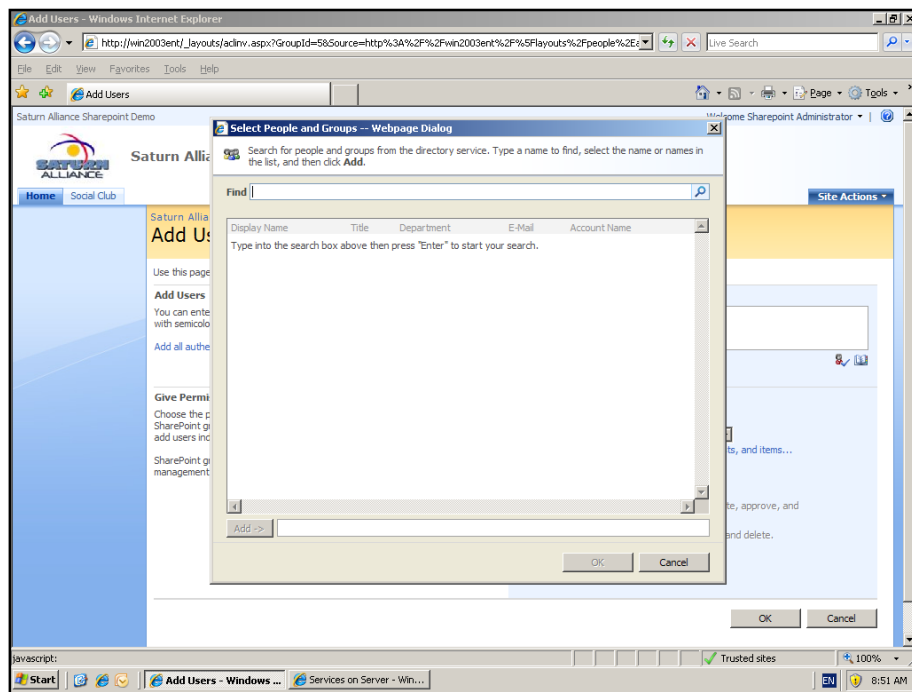
If you are unsure of the user details you can press the *Select People* icon, which is also in the lower right of this box (and appears like an open book). When pressed, you will see a window like that shown above. Simply enter the details of the user and press the **Find** button.
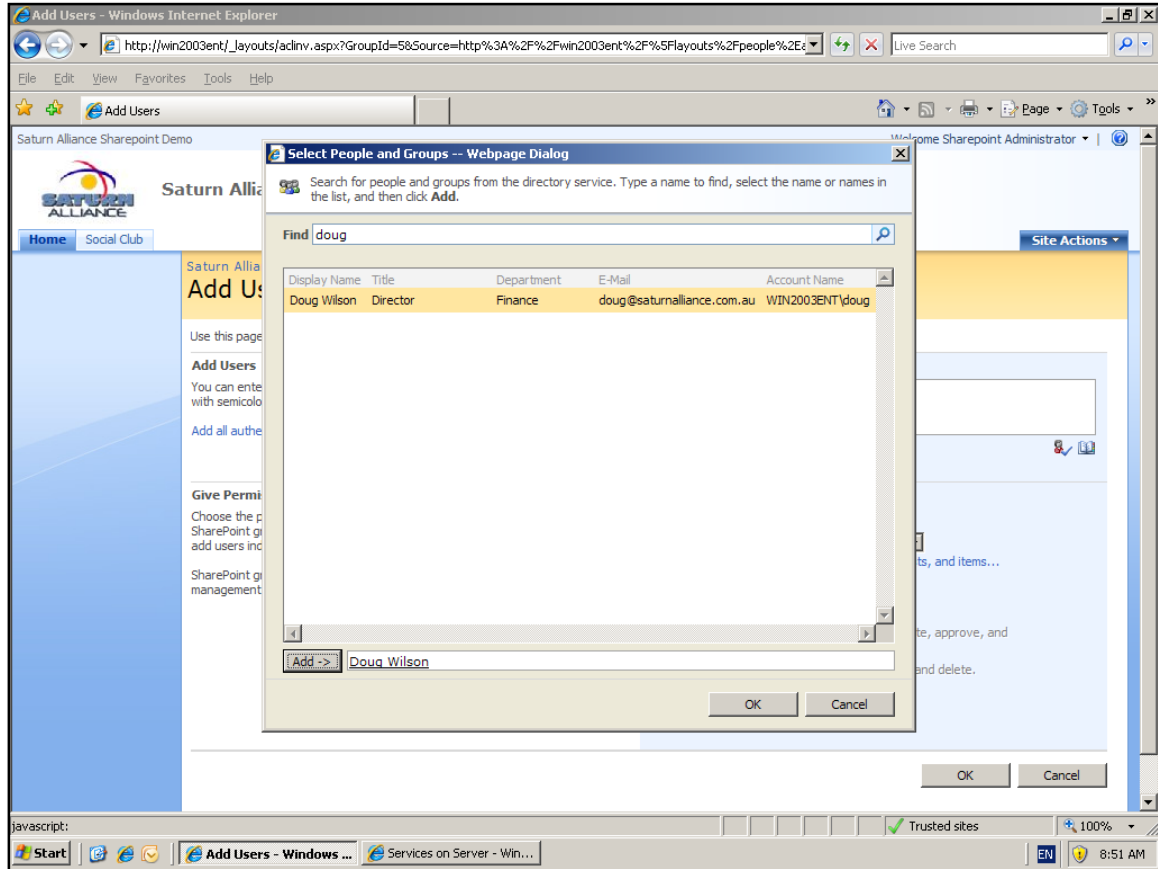
If that user can be located on the network then it will be displayed in the lower part of the window. Simply select the user and press that **Add** button at the bottom of the screen so the name appears next to the *Add* button. Press **OK** when you have completed finding all the users.
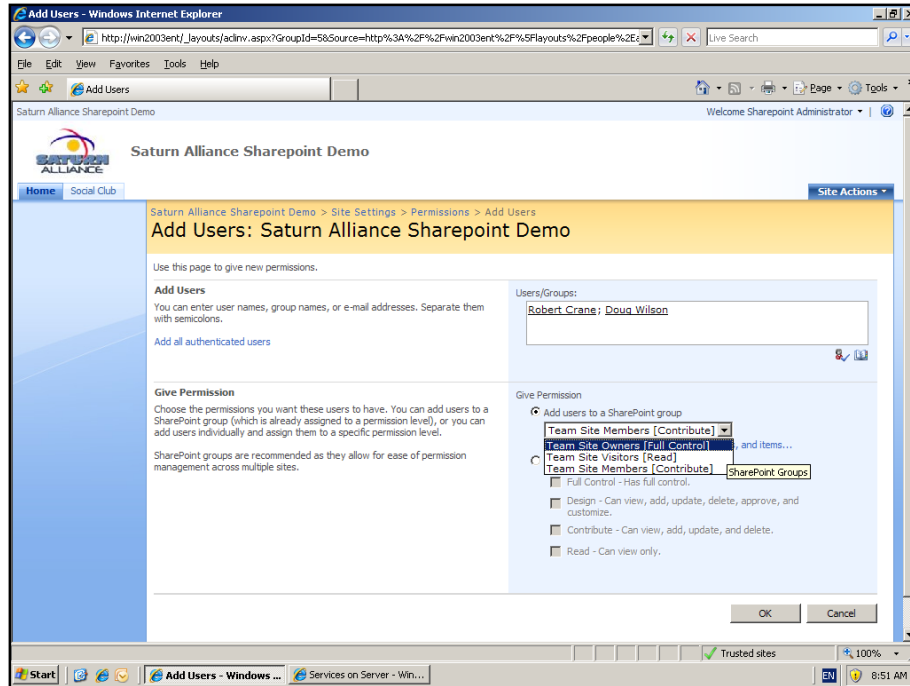
Once you have selected the users you wish to add you can now select whether you wish to add the users to an existing WSS v3 group or configure these rights manually. It is normally best practice to add users to WSS v3 groups and assign rights to these groups throughout the site.

If you enabled outgoing emails in WSS v3 (see **Chapter 9 – Advanced Configuration**) you will also be prompted to send an email to the user.
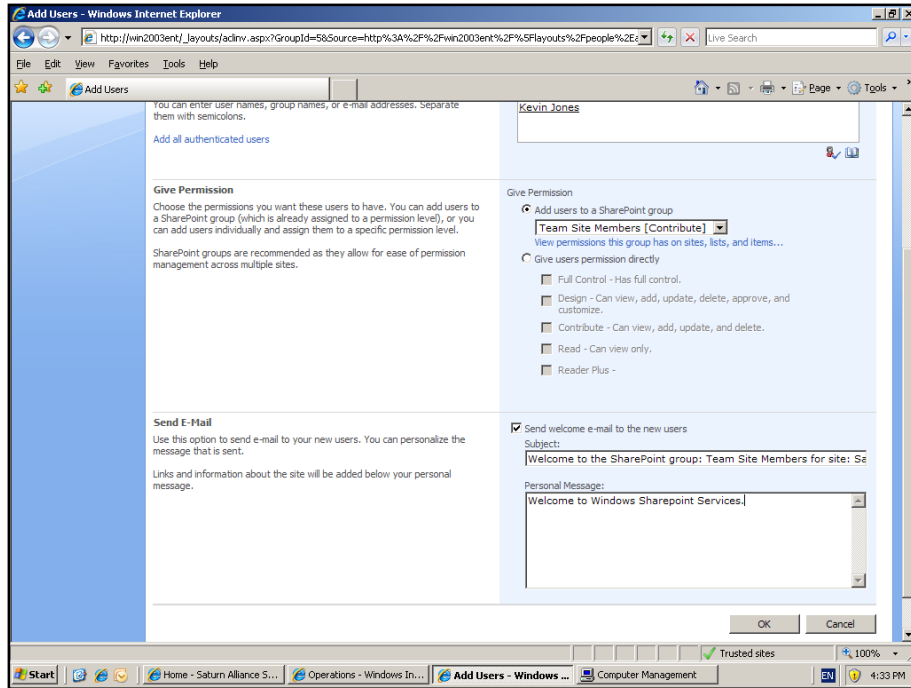
The email address for this network user must be correctly configured along with the outbound WSS v3 settings otherwise you will receive an error.

Once you have completed assigning rights press **OK** to continue.
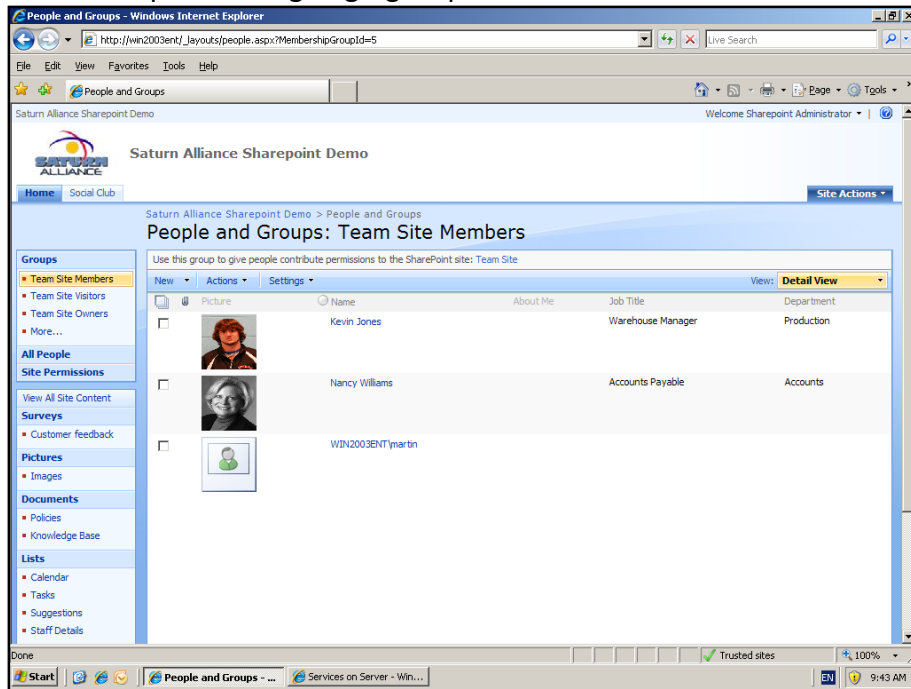
The users you added should now appear under the respective groups you allocated. To view and edit the details of a user simply click on their name or photo (if it exists).
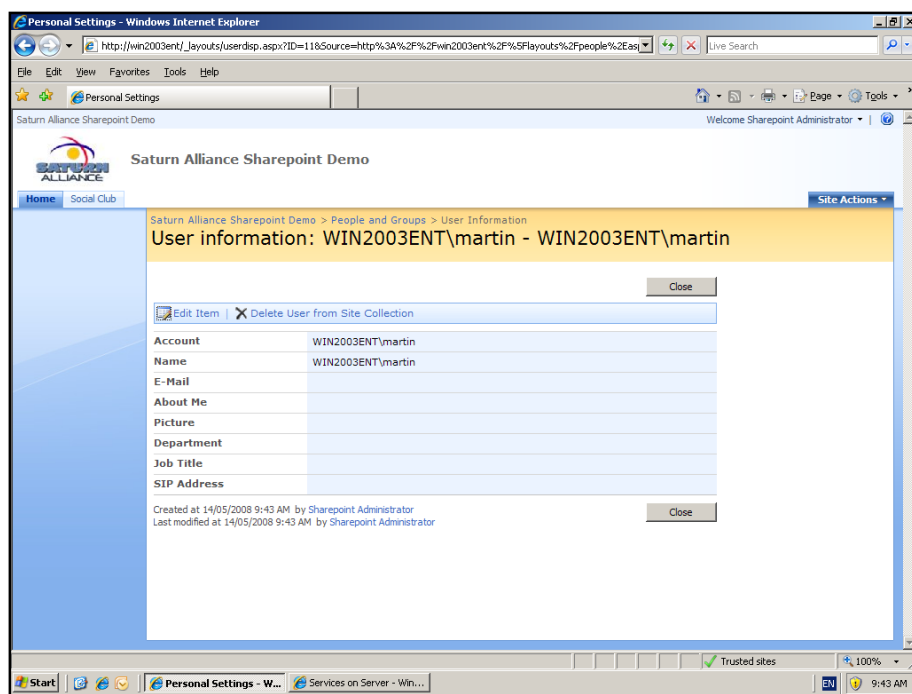
Once you click on the user you are able to go in and edit their details by selecting **Edit Item** from the menu.
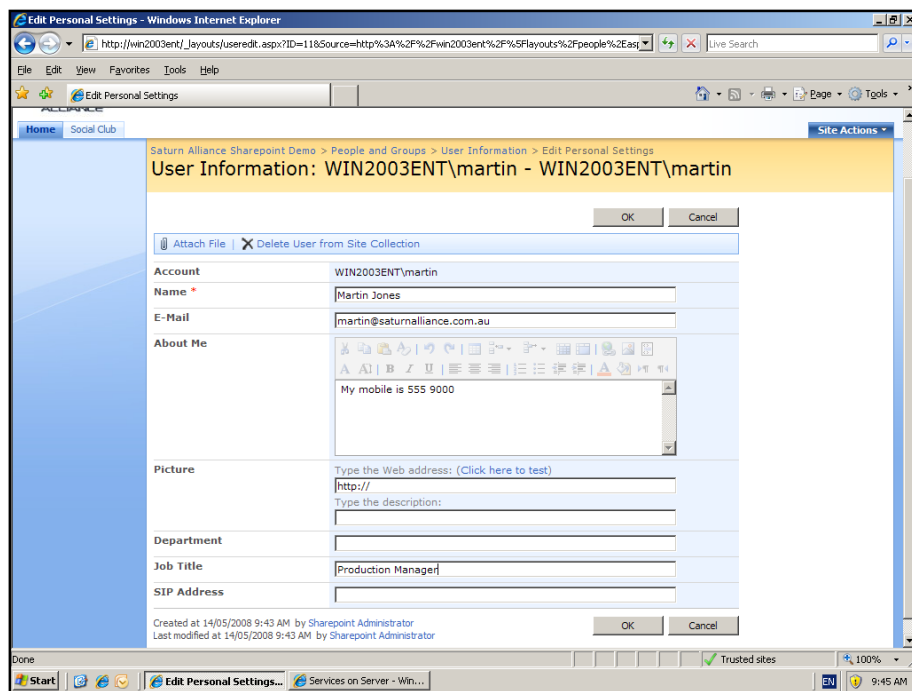
Once you have completed editing the information press **OK** to save and continue.
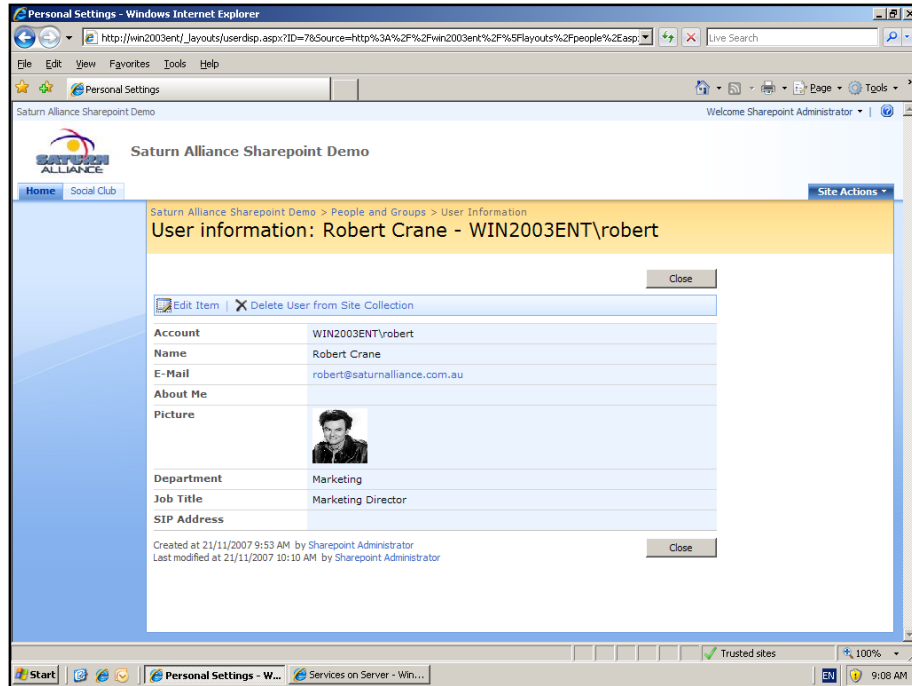
It is also possible to delete a user from WSS v3 here by simply clicking the **Delete User from Site Collection** on the menu bar.

15.5   WSS v3 permissions
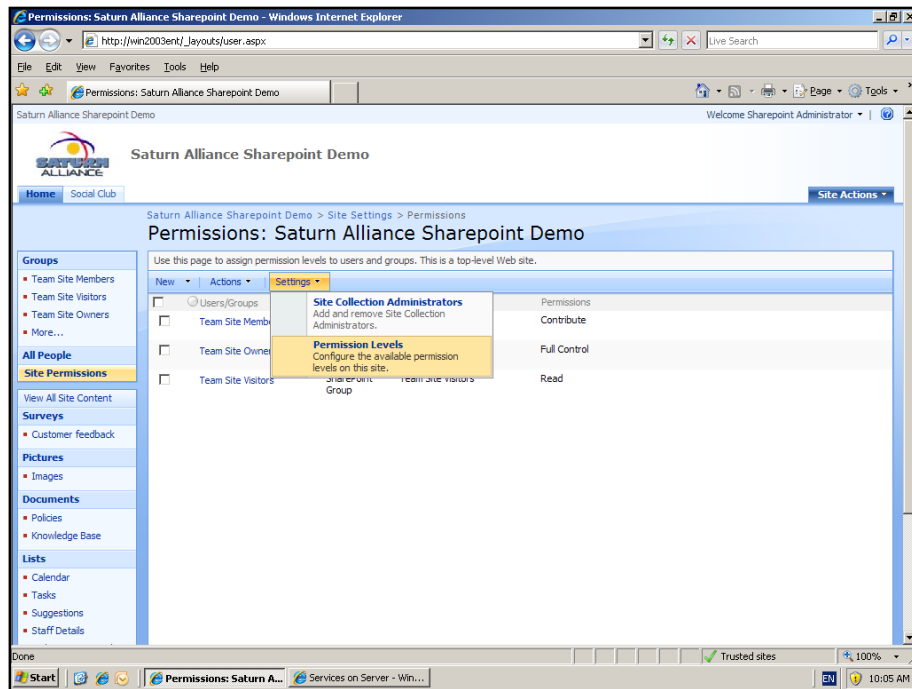
It is best practice not to make changes to the standard WSS v3 groups as this may cause confusion at a later stage. A better idea is to create new groups with the desired rights based on an existing group.

To create a new WSS v3 group select **Site Permissions** from the *Quick Start* menu and then select **Settings | Permission Levels** from the menu bar.
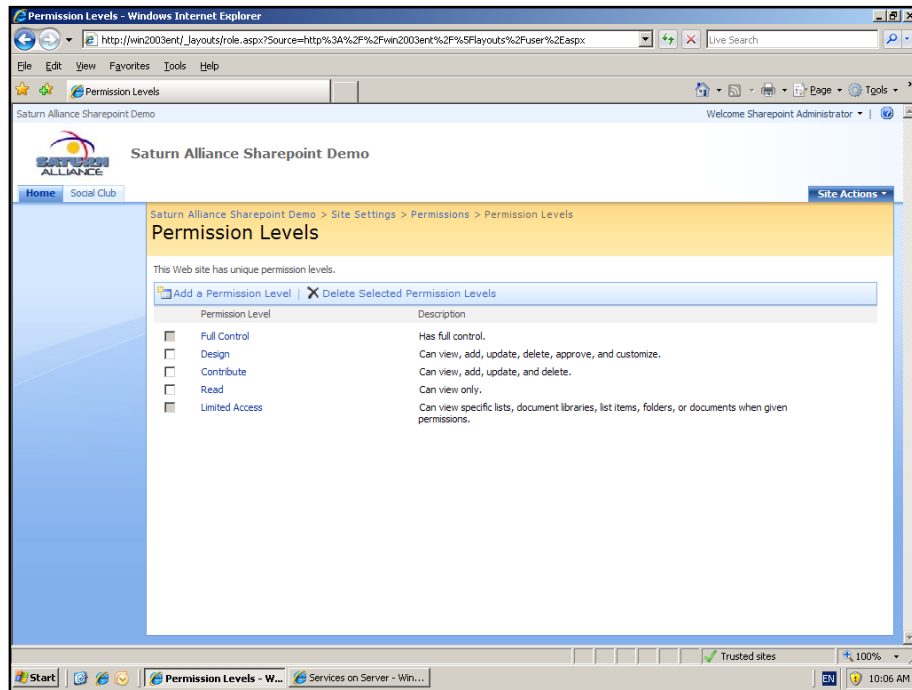
You will now see a list of existing WSS v3 permissions. If we wish to base our new group on the existing *Read* permissions select this from the list by clicking on the word **Read**.
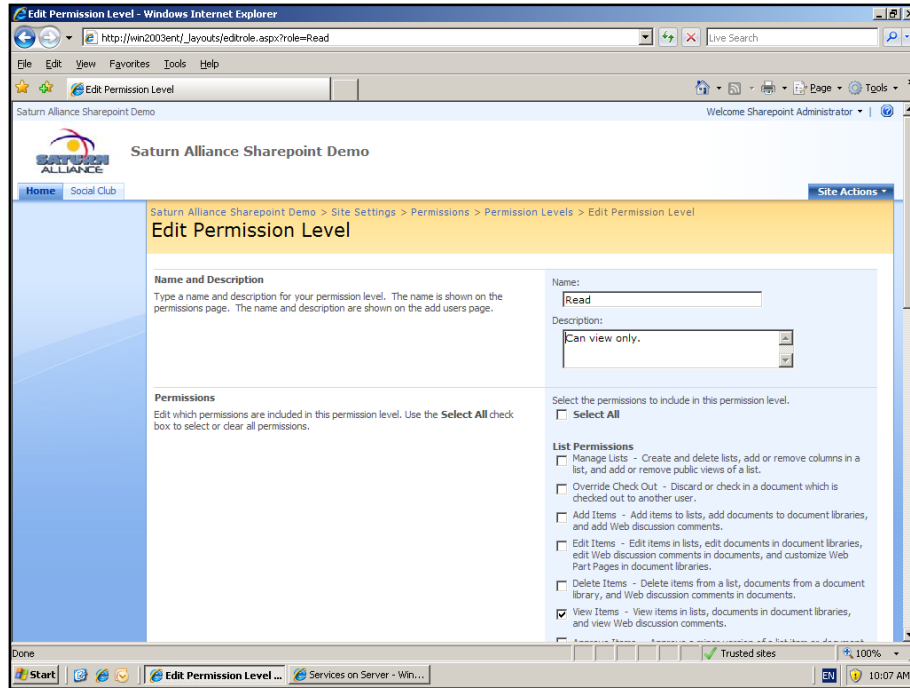
This will now show you all the rights the Read permission has. Scroll down to the bottom of the page.
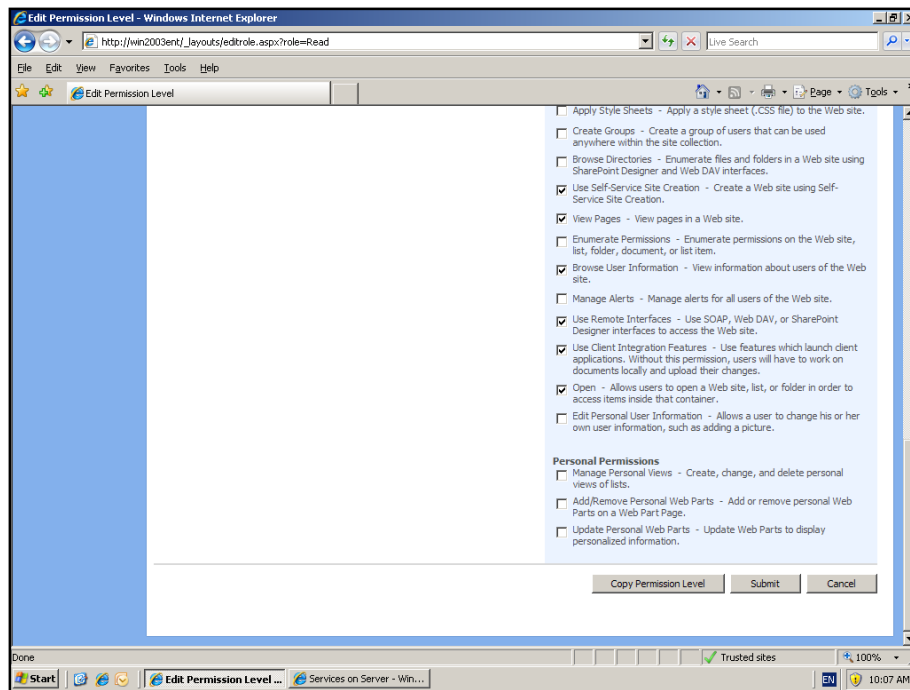
Here you will see a *Copy Permission Level* button. Press this to make a copy of this.
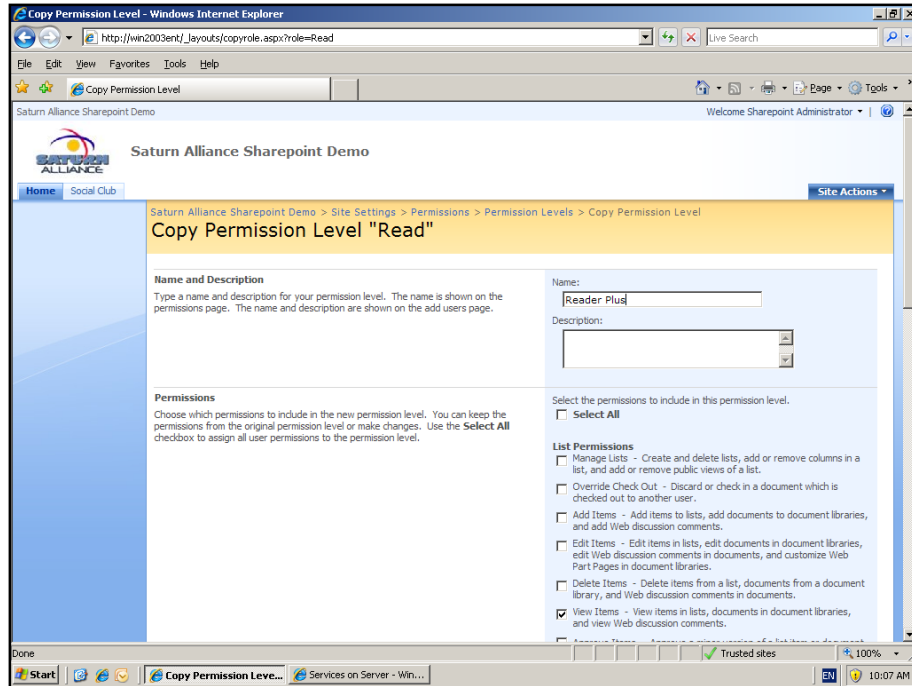
Give the new permission an appropriate name and then the appropriate rights. As you scroll down the list you will see the list of permissions that have already been copied from the previous permission level.
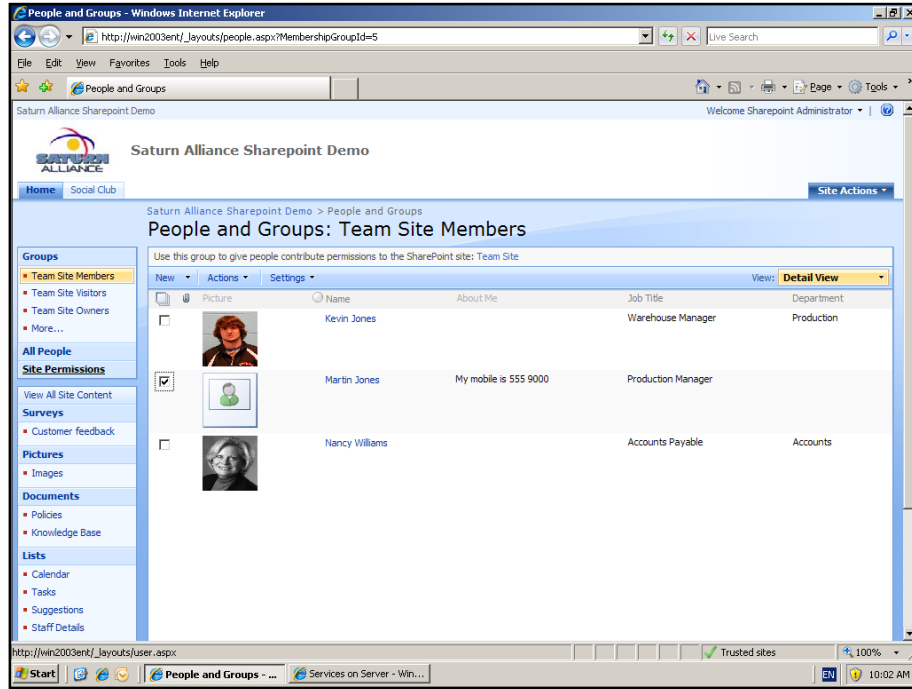
When you have completed your selection press the **OK** button at the bottom of the screen to continue.
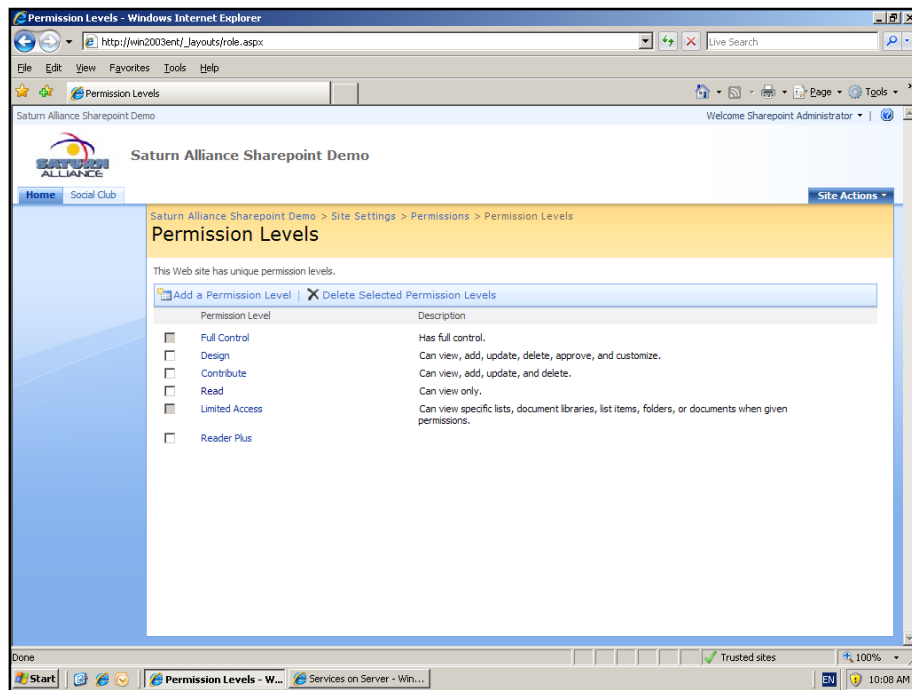
You should now the new permission in the list as shown above.

15.6   WSS v3 Groups

To create a new WSS v3 group select **Site Permissions** from the *Quick Start* menu.
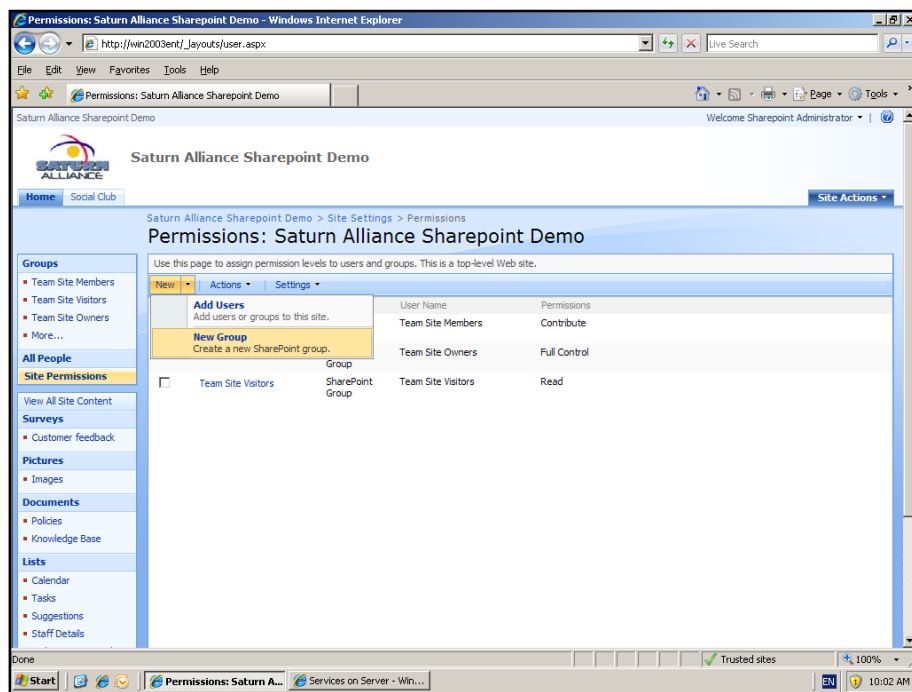
You should now see the list of WSS v3 groups. To add a new group select **New | New Group** from the *Menu bar*.

Complete the information about the new group, like the name, owner and its group settings. Scroll down the screen for more options.

At the bottom of the list you will see all the WSS v3 permissions that are available. As mentioned previously it is best practice to create new permissions rather than change any existing WSS v3 permissions. After this you can assign these new permissions to the new group you are creating.

When complete press **Create** to continue.
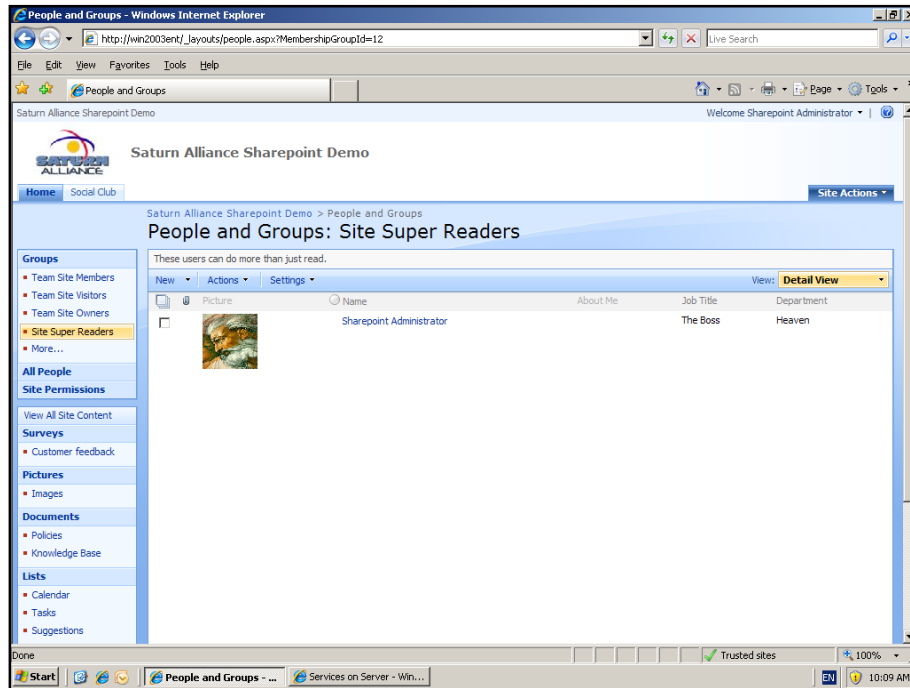
The new group is now displayed, the only member will be the group administrator you specified previously. You can add users to this group by selecting **New | Add Users**.
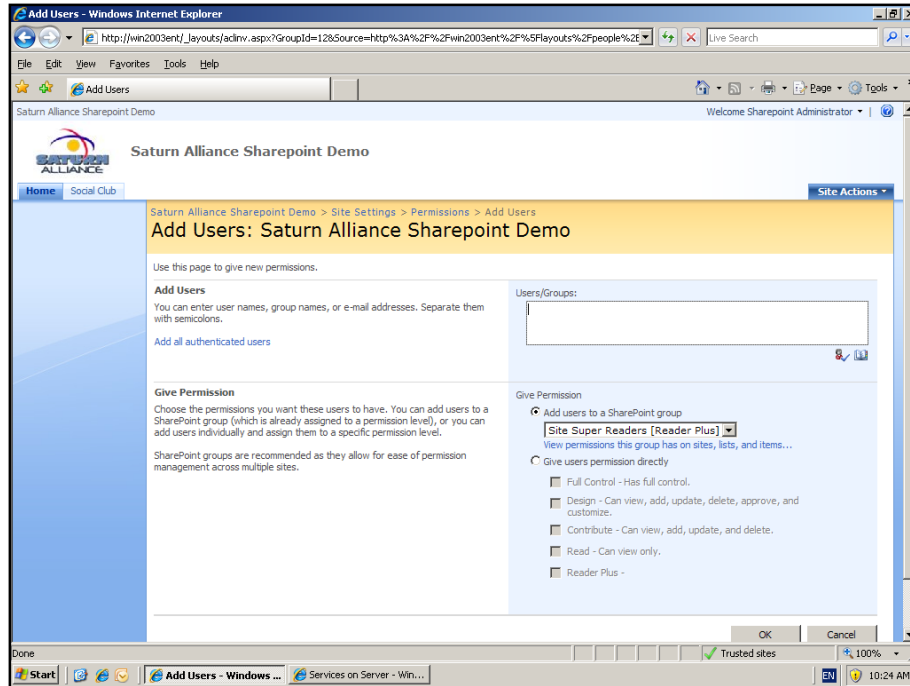
Add the desired network users to the upper window and select **OK** to continue.

15.7 Enabling anonymous site access

Any anonymous access to WSS v3 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 WSS v3 permissions but initially the site must be enabled for anonymous access (since it isn't by default).
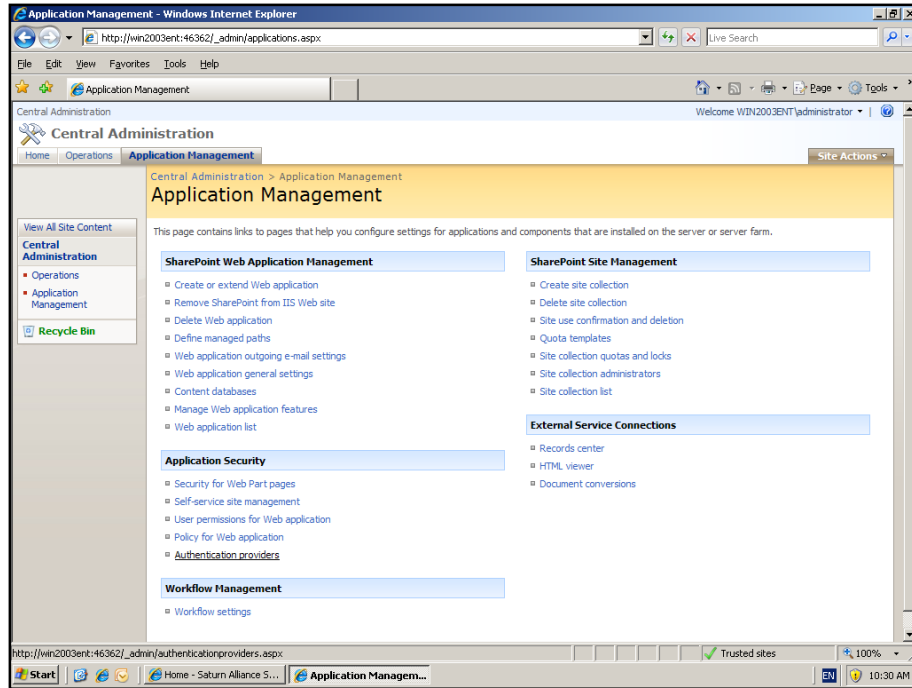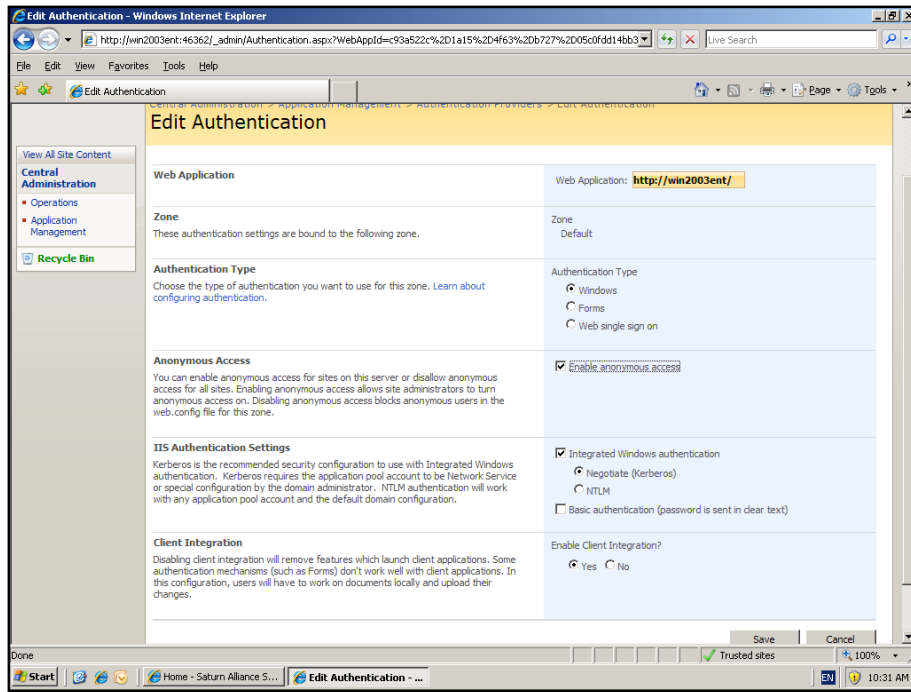
To allow anonymous access logon to the Windows SharePoint Services Central Administration. On the *Application Management* tab under *Application Security* select **Authentication Providers**.
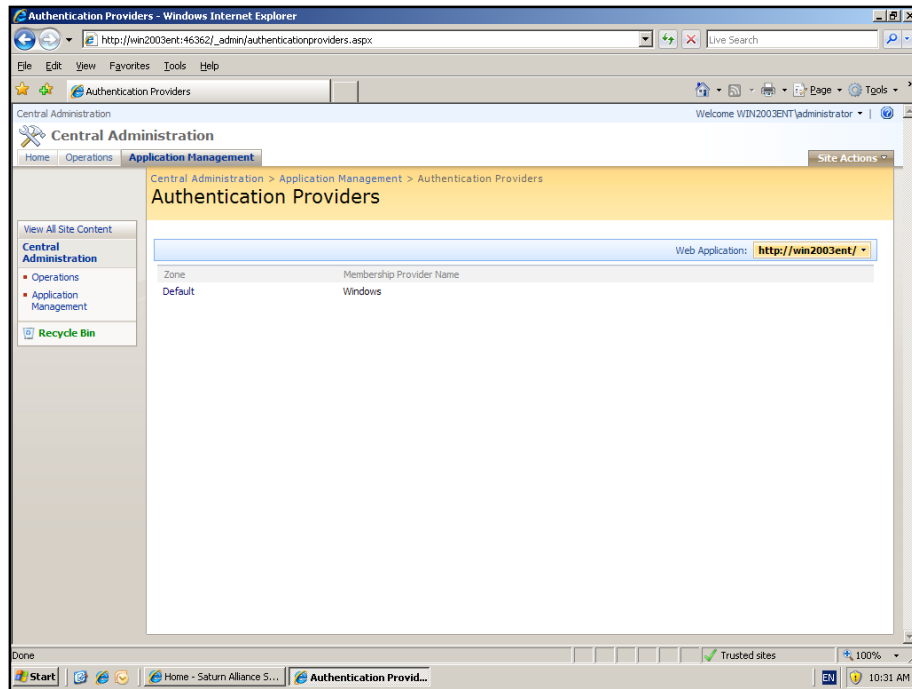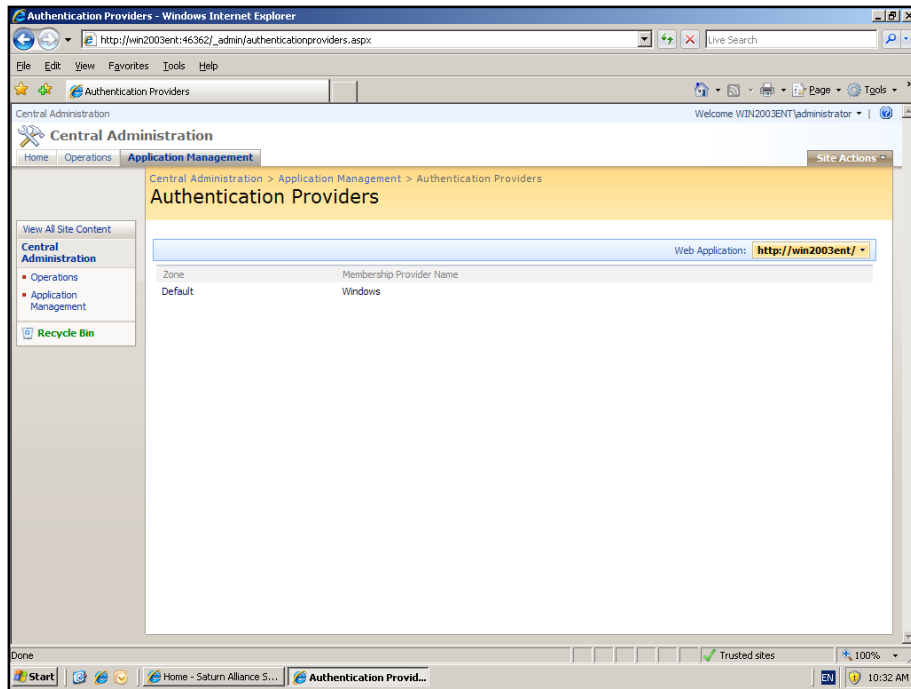

Click on the *Default* Zone.

Locate the option under the section *Anonymous Access* and click to enable it. Select the **Save** button at the bottom of the screen to save the changes.

You will be returned to the Authentication Providers screen.

Since WSS v3 is a web application that uses Internet Information Services on the host Windows Server where you are running WSS v3 anonymous access also needs to be granted here. By going through the above process the necessary steps have been completed by WSS v3. To check this, log in to the WSS v3 server as an administrator and select **Start** | **Administrative Tools** | **Internet Information Services Manager**.
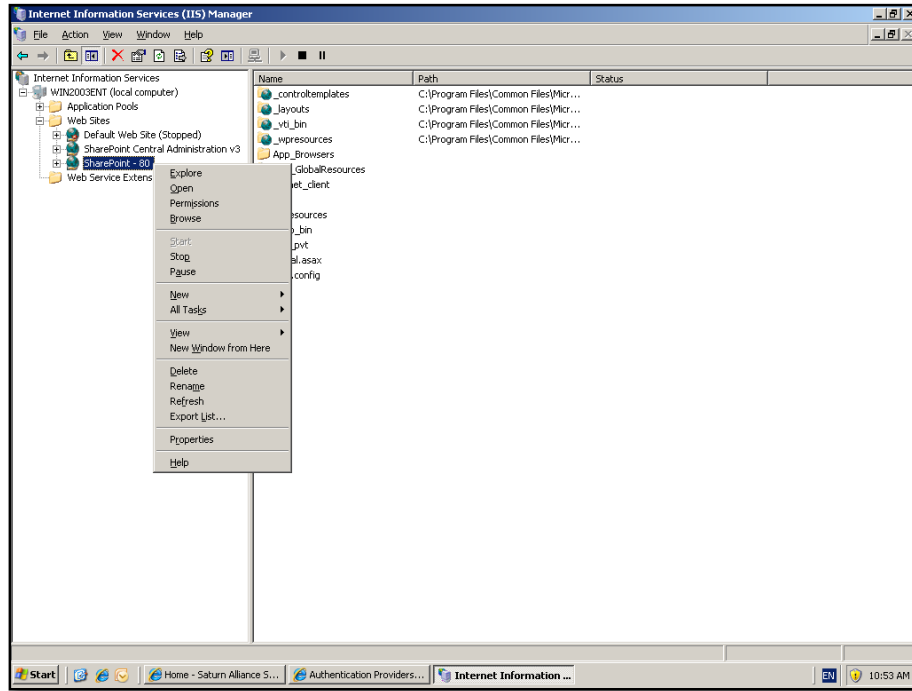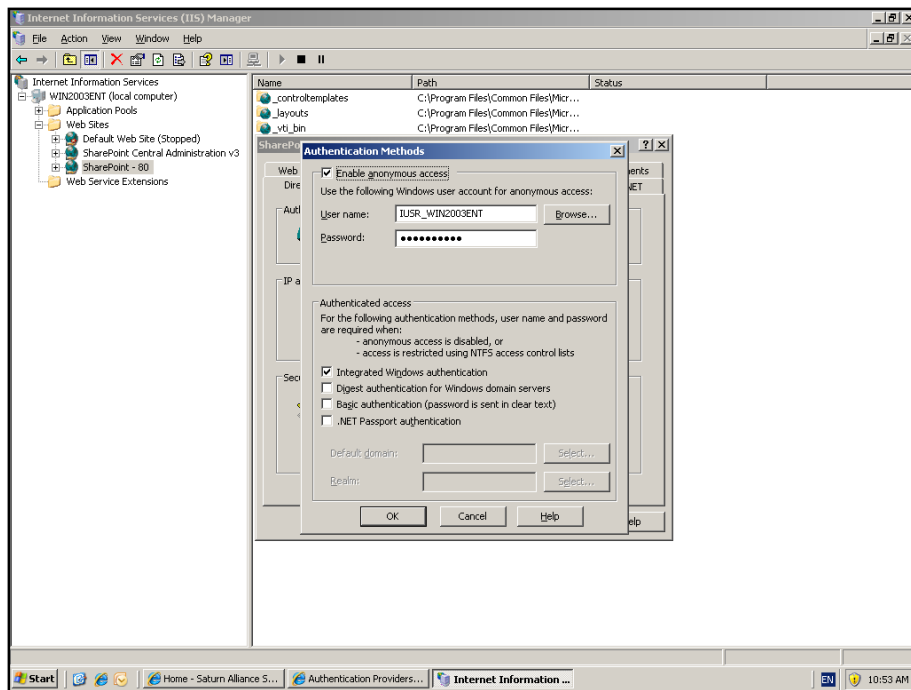

Locate the WSS v3 site under the W*ebs Sites* folder (here it is called Sharepoint – 80). **Right mouse click** and select **Properties** from the menu that appears.
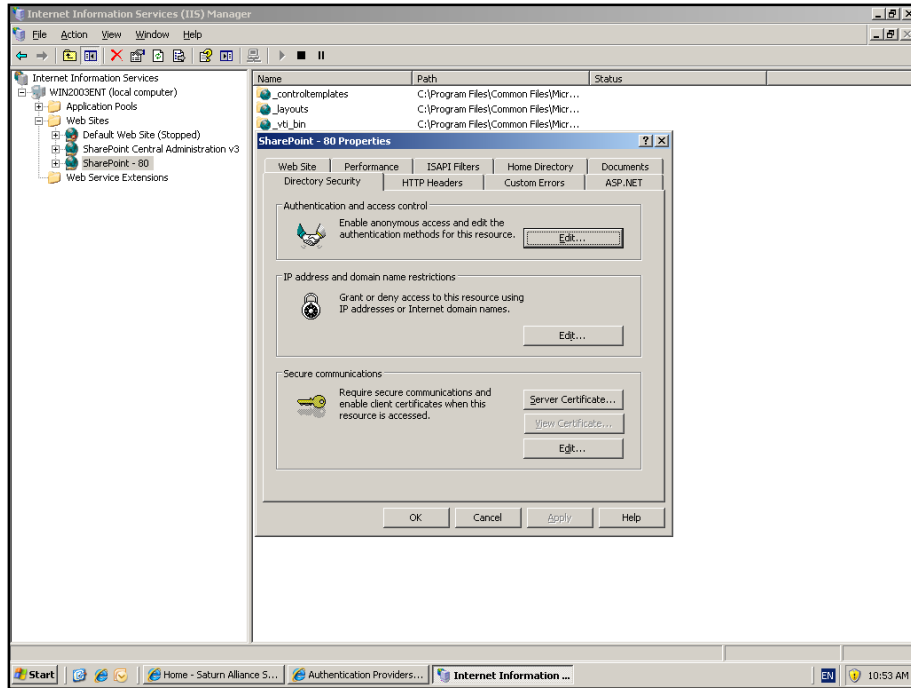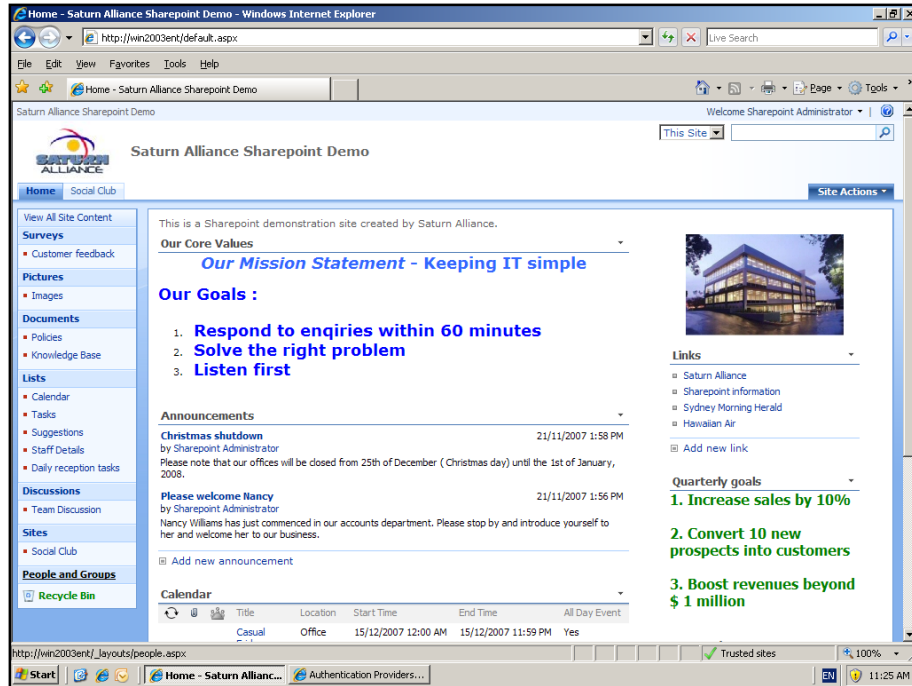
Locate the *Directory Security* tab and click the **Edit** button in the *Authentication and access control* section.
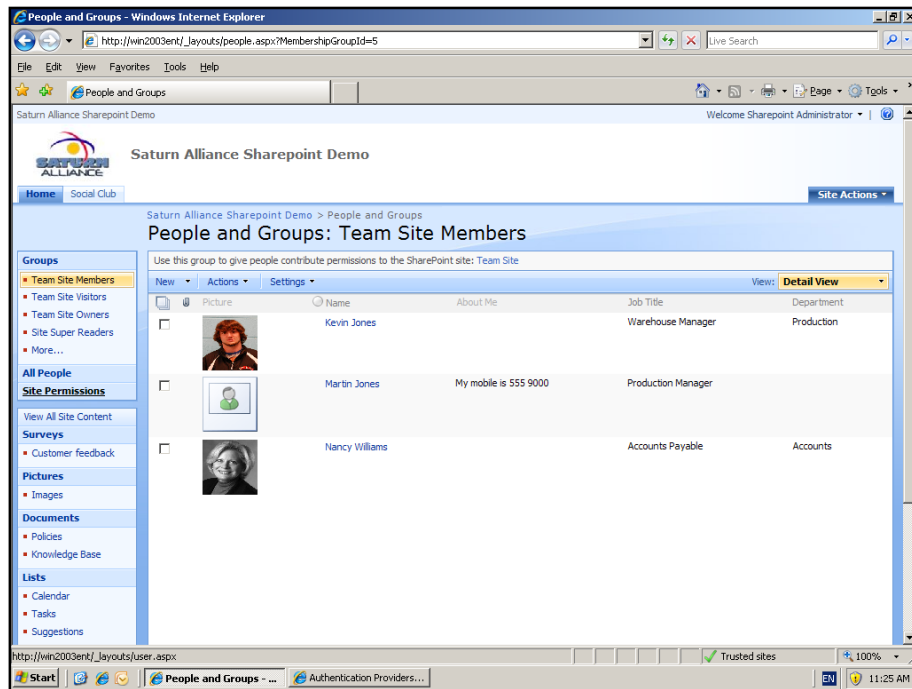

You should see that anonymous access is enabled for this site.

Now that the WSS v3 web application has been enabled for anonymous access it also has to be enabled on each WSS v3 site. To do this simply login to the WSS v3 site as an administrator then select **People and Groups** from the *Quick Start* menu on the left hand side.
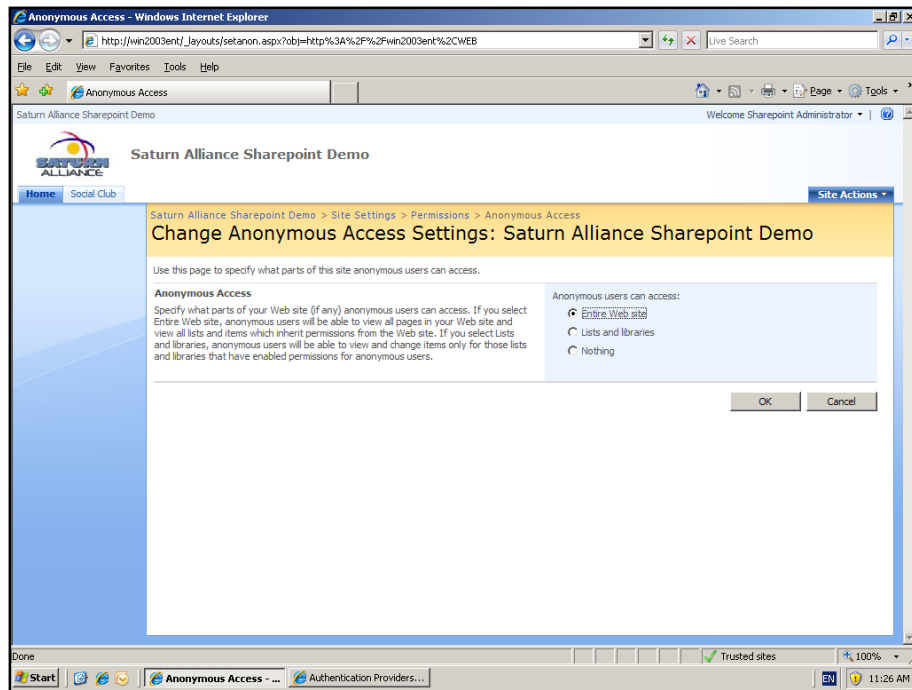

Now select **Site Permissions** from the *Quick Start* menu.
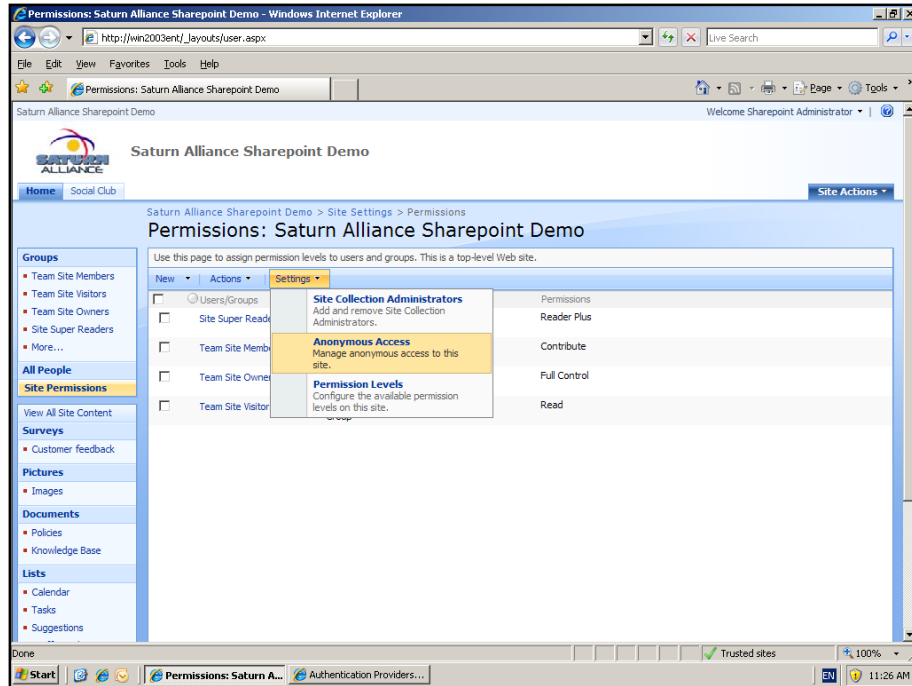
Now select **Settings** | **Anonymous Access** from the menu bar.

Select what level of anonymous access you wish to enable. The options are:

> *Entire Web site:* any user can access any part of the WSS v3 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.
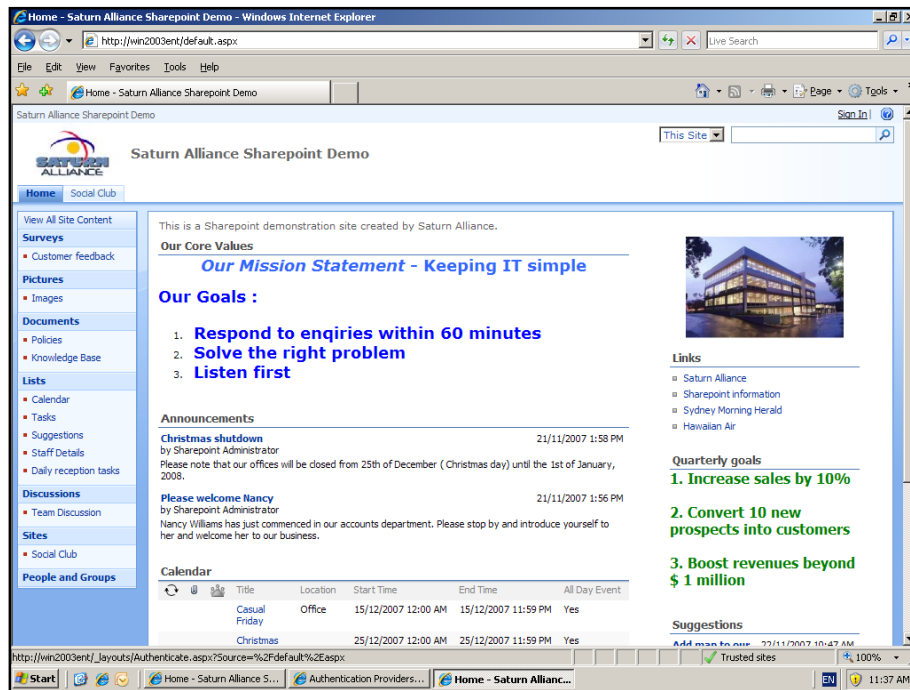
If you now open a new browser window and access your WSS v3 site you should find that it is displayed as normal. However, in the top right of the screen you will see that instead of being logged in as a network user you are not logged in (denoted by *Sign In*).
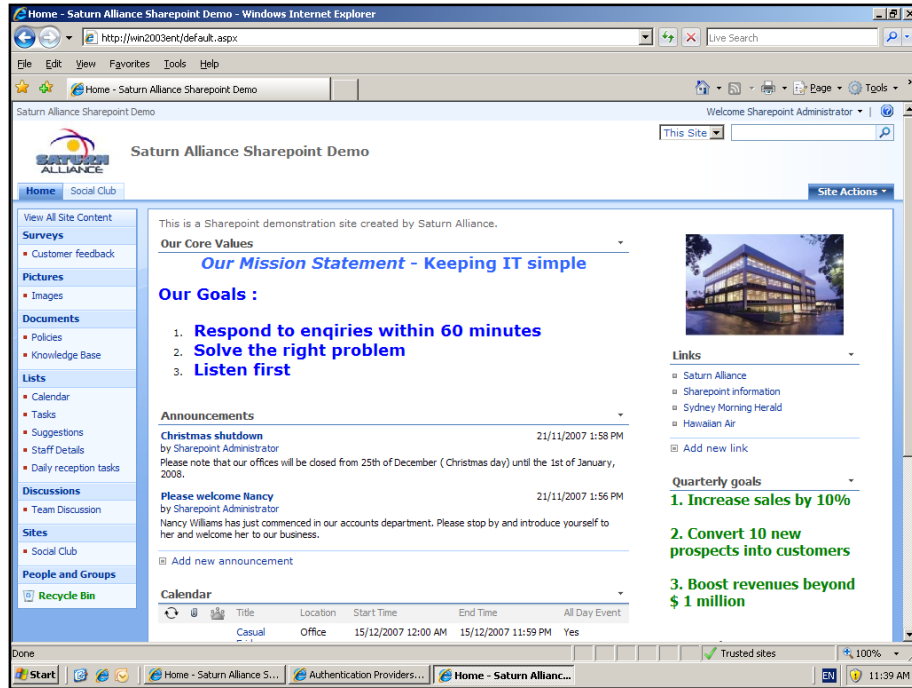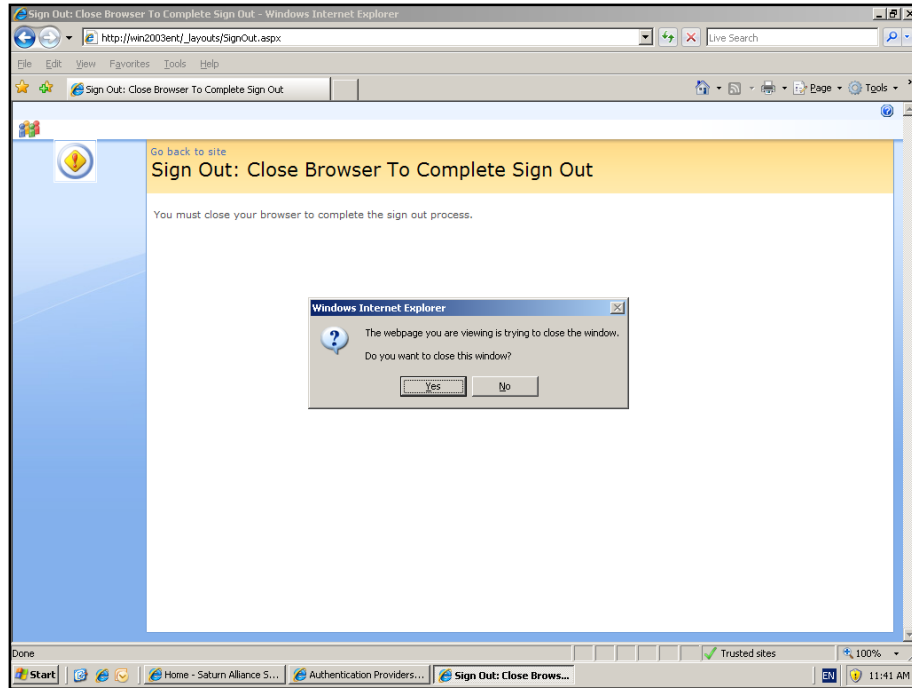
If you click the **Sign In** link you will automatically be logged into WSS v3 as the current network user.
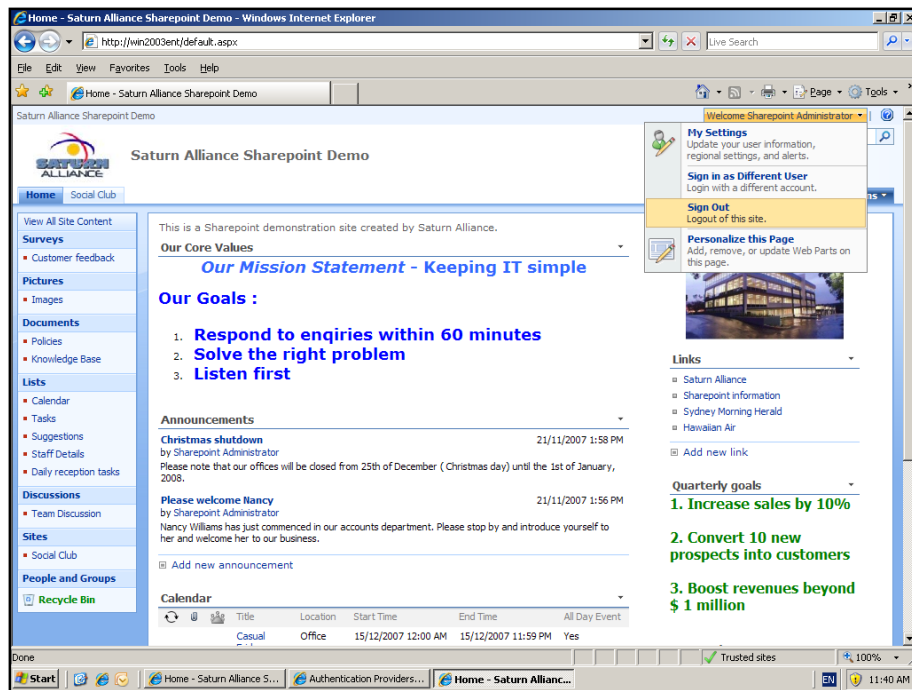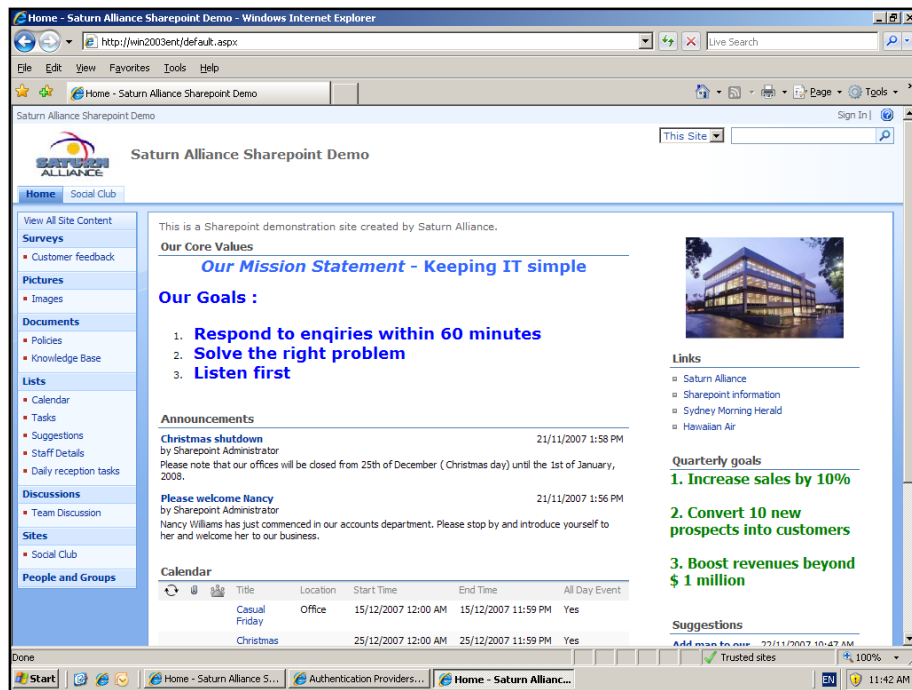

If you pull down the arrow to right next to the login name you are able to select the option from a menu to **Sign Out**.
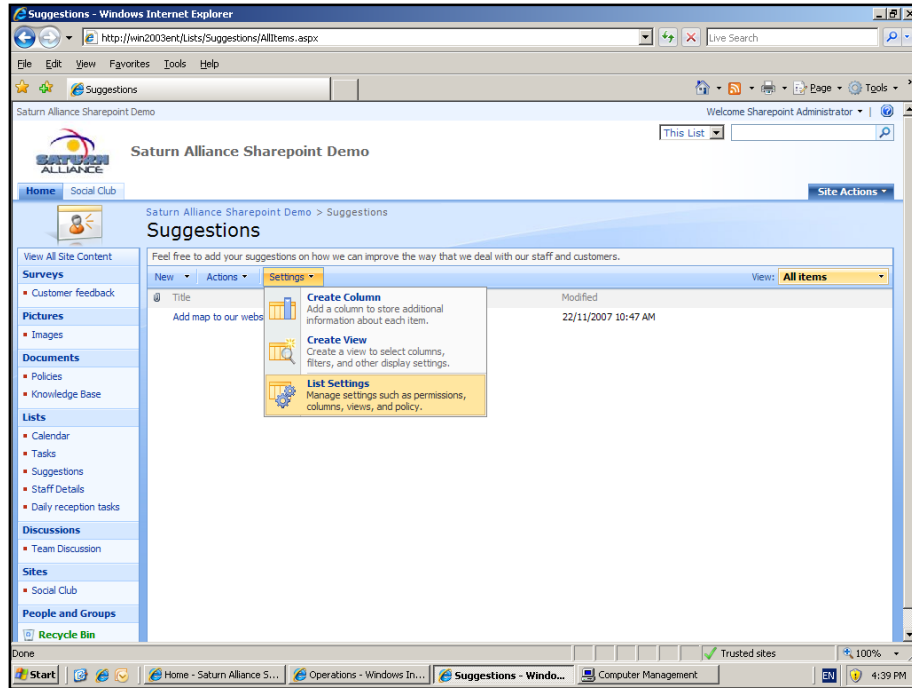
You will be signed out of the site. If you return to the WSS v3 site again in your browser you will see that you are no longer logged in.

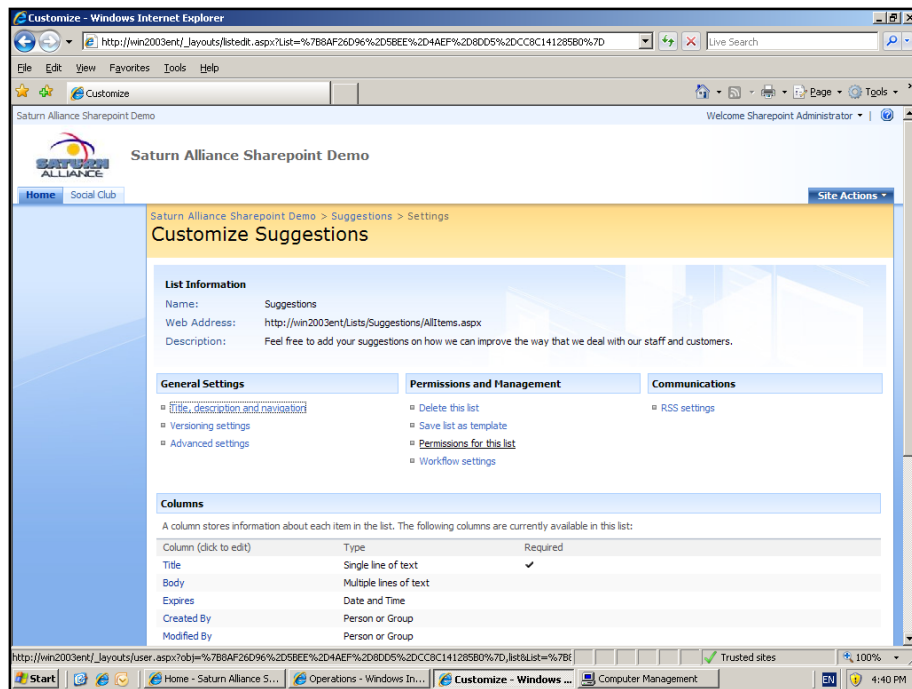You must again select *Sign in* the top right of the window to log in as a network user to this WSS v3 site.
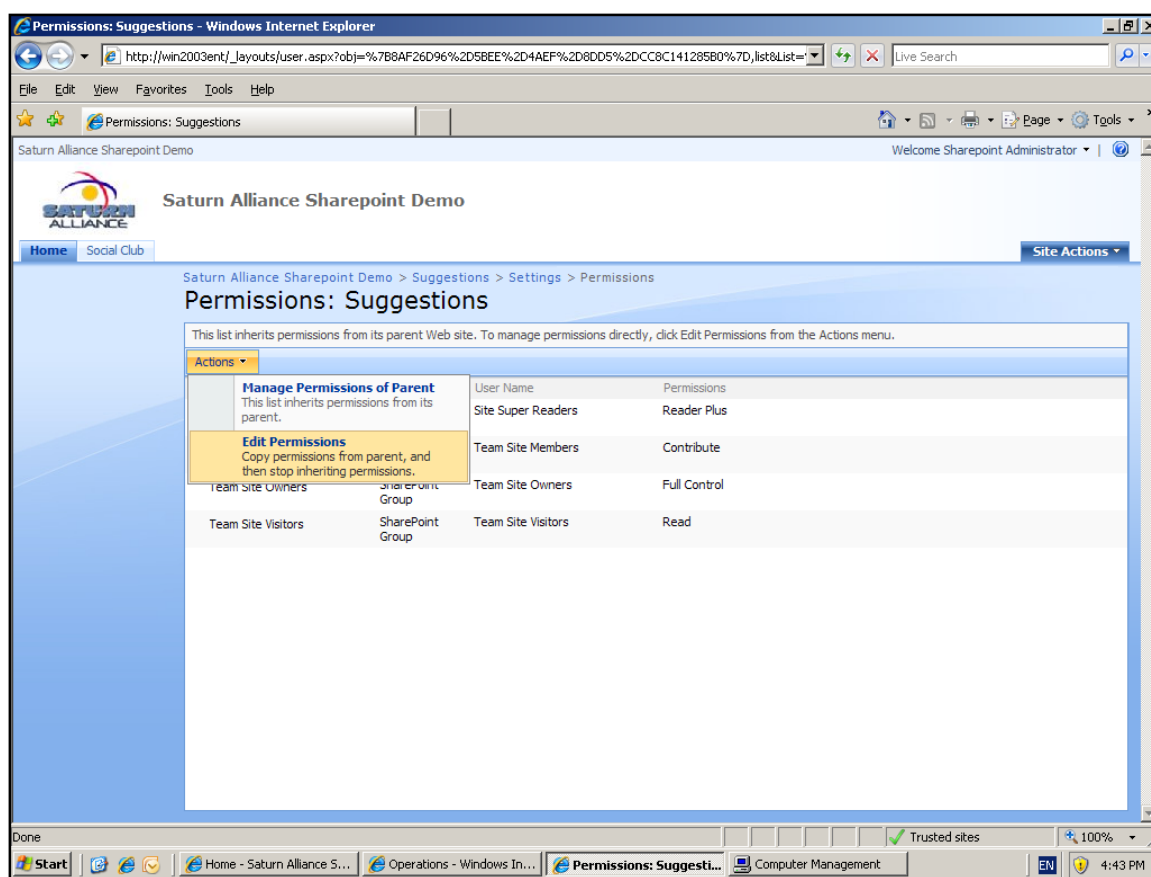
Finally, you need to allow anonymous access to the items in WSS v3. To do this, for example on an existing list, go to the list and select **Settings** | **List Settings** from the menu bar.

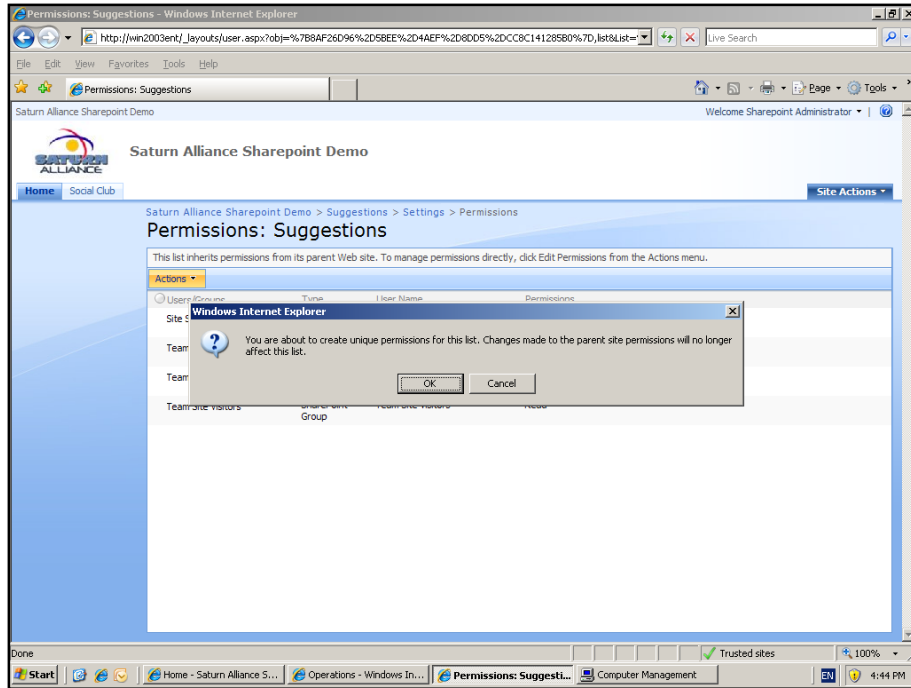In the list settings select **Permissions for this list** from *Permissions and Management* section.

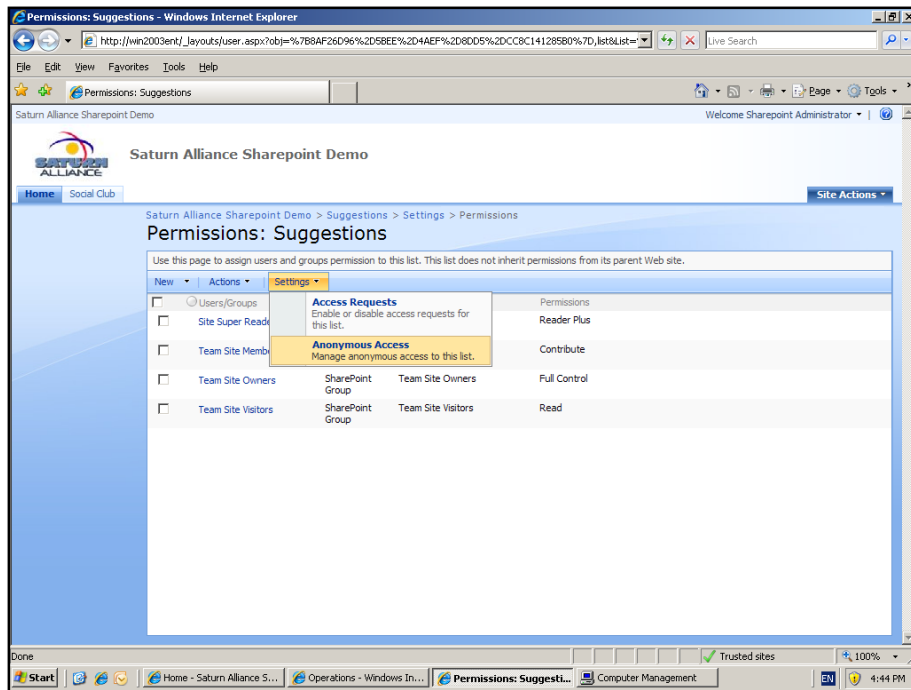By default, the list will normally inherit its permissions from the parent site. To prevent this select **Actions** | **Edit Permissions** from the menu bar.
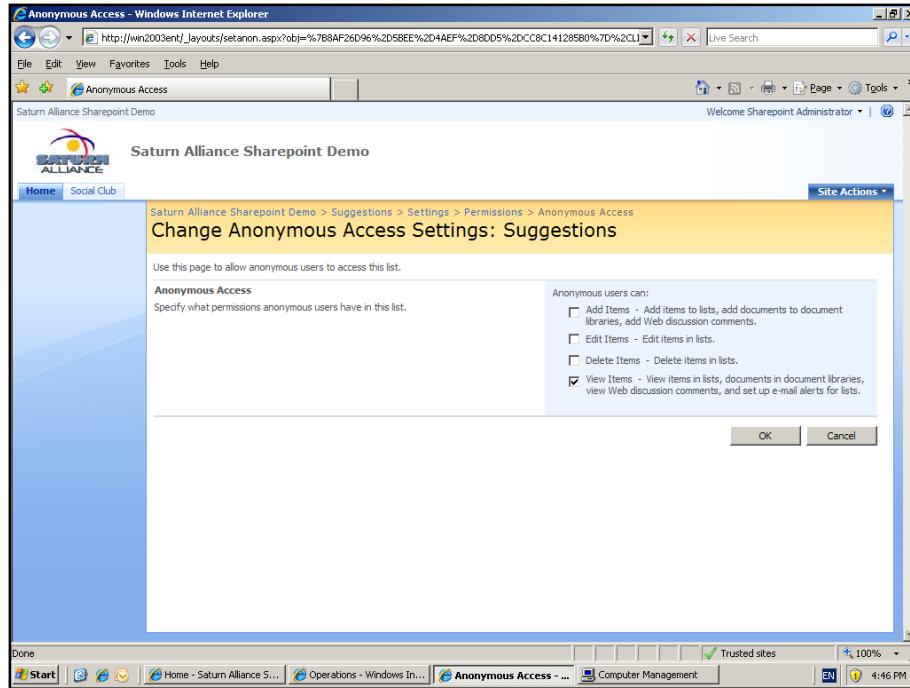
Press the **OK** button to accept the changes and continue.

You will be returned to the Permissions window. You will notice that menu bar now contains a number of additional options. To enable anonymous access select **Settings | Anonymous Access** from the menu 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).

15.8   SharePoint elements security

SharePoint security operates in a manner very similar to that found on normal files and folders. It is generally the case that security rights are inherited and flow down through the SharePoint site structure. This means that unless explicitly set, anything you create will have the same rights as that of its parent. Thus, if you create a new Document Library it will, by default, have the same rights as the site in which you created it. This does not mean that these rights can't be changed but this is generally how security is assigned by default.

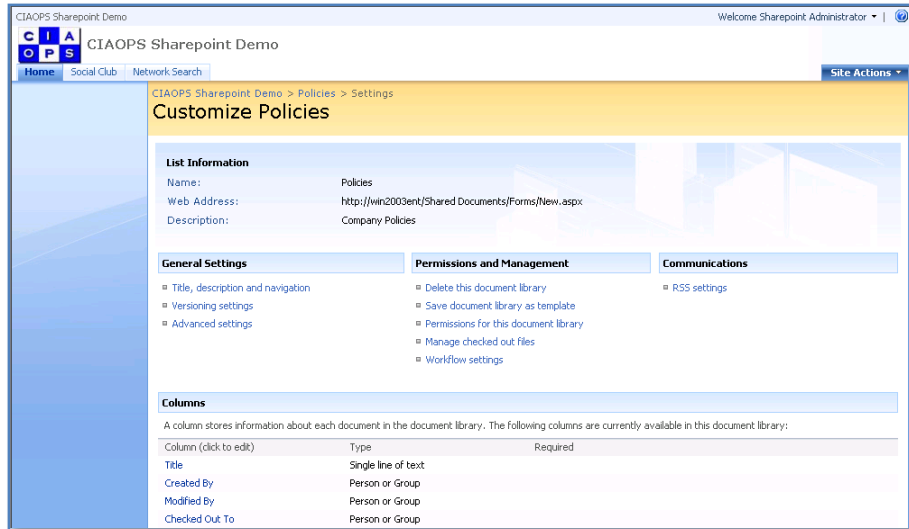The following example will take your through changing the rights in a Document Library.
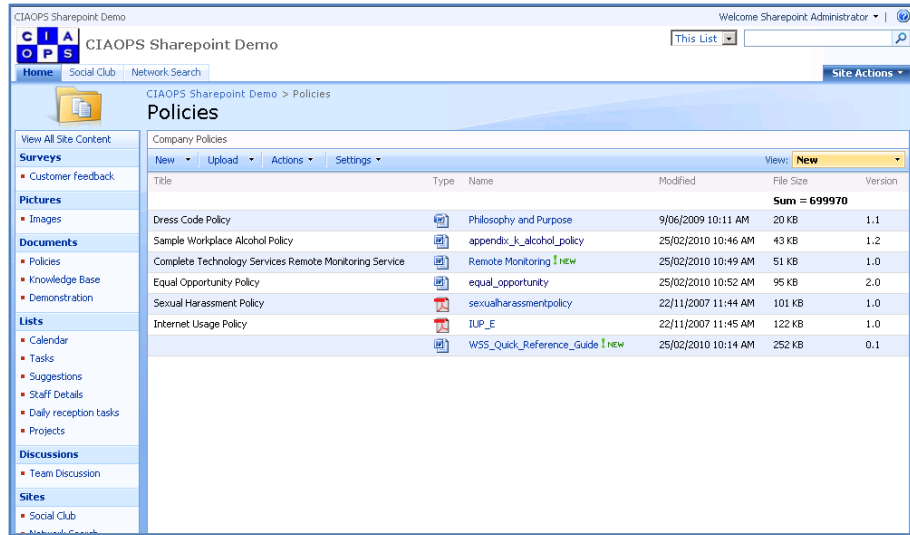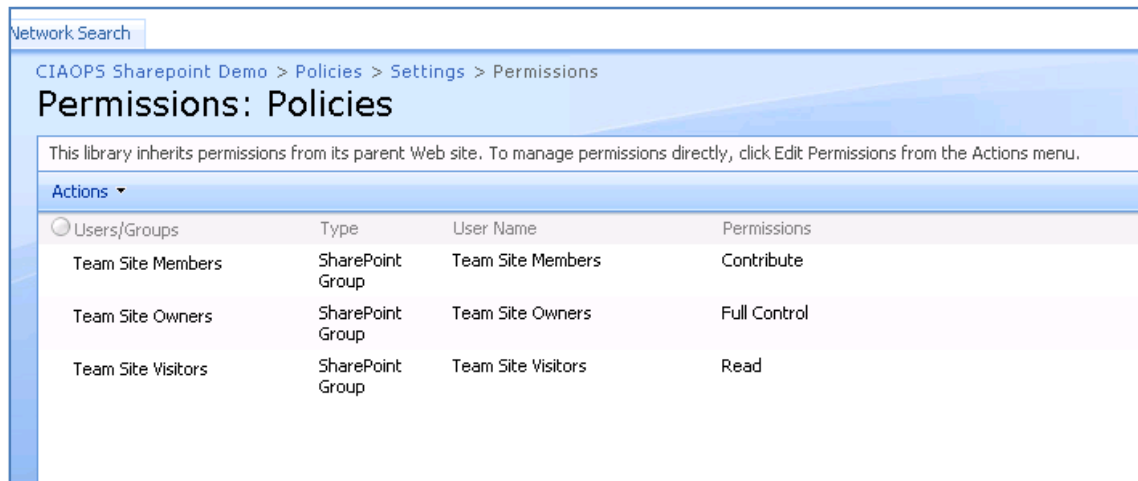
Firstly, go to the Document Library using the browser.
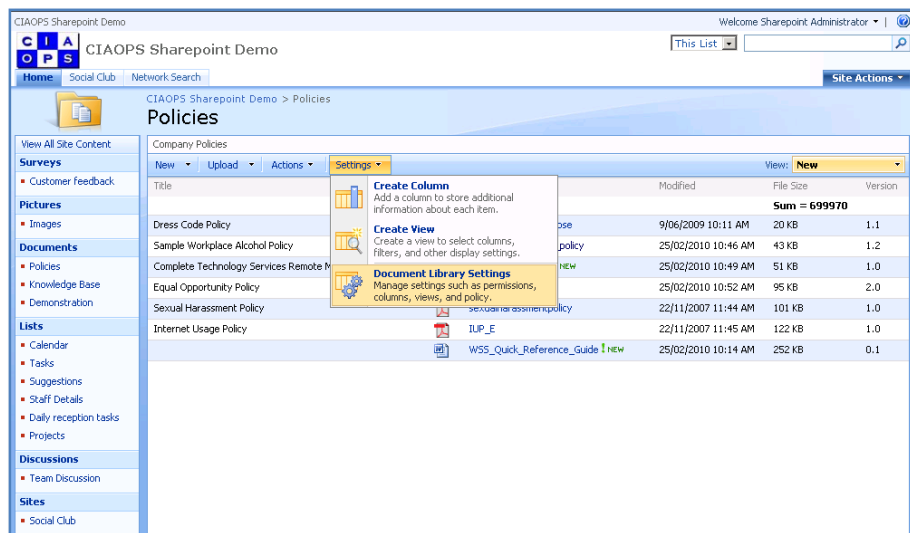
From the Document Library menu select **Settings** then **Document Library Settings**.

From the section *Permissions and Management* in the centre of the page select **Permissions for this document library**.

You should now see the securities for the Document Library as shown above. Here you will notice the information line just above the *Actions* option on the menu – "*This library inherits permissions from its parent Web site. To manage permissions directly, click the Edit Permissions from the Action menu*".

This means that the securities for the Document Library are being inherited from the parent site.
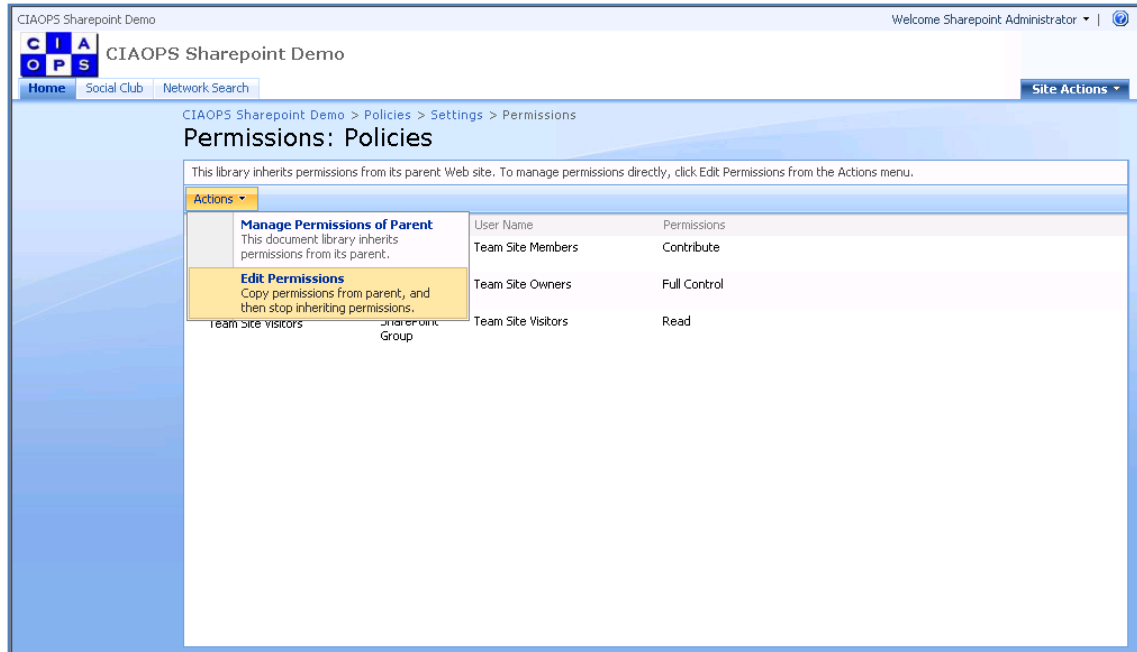
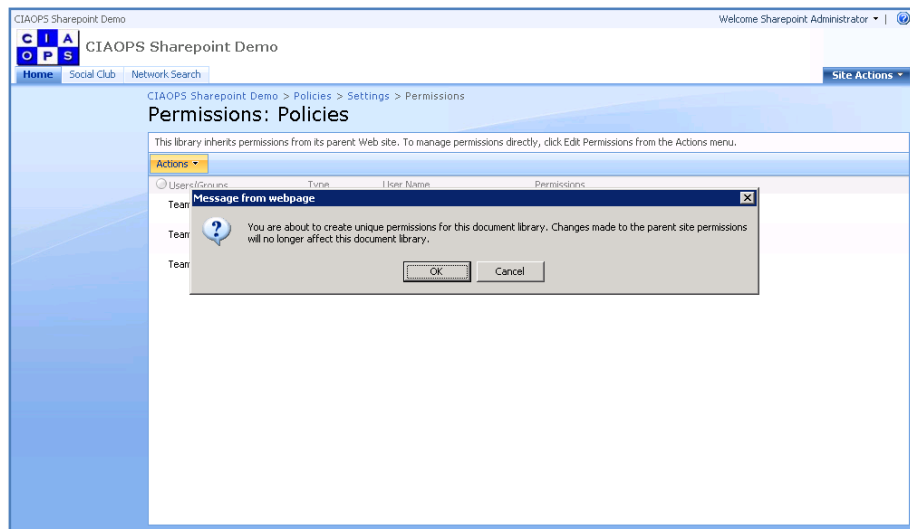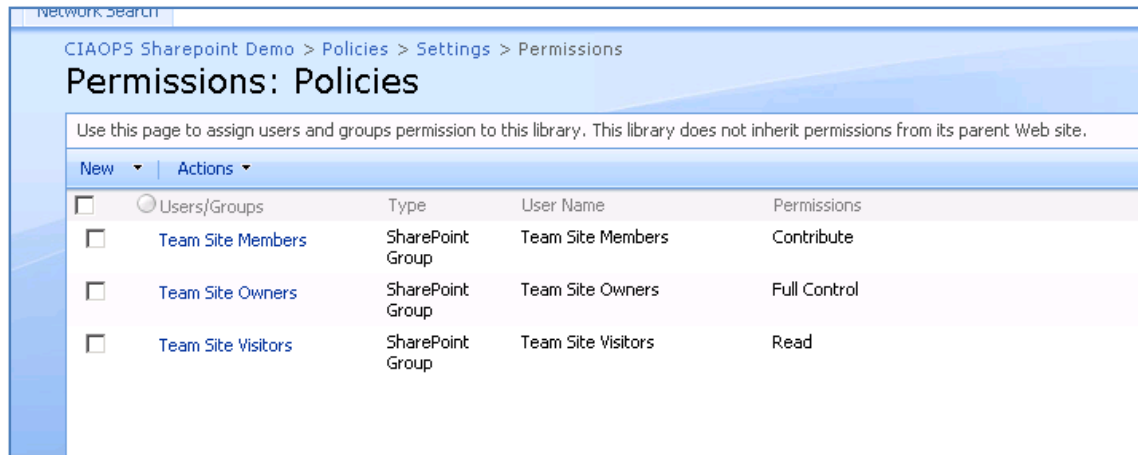Since we wish to change the permissions here select **Actions** then **Edit Permissions**.

You are now prompted with a warning that are about to break the inheritance of the Document Library and create unique permissions.

Press **OK** to continue.

You will now be returned to the *Permissions* window but you will notice a number of changes. Firstly you will see that the informational line above *Actions* on the menu bar now reads – "*Use this page to assign users and groups permissions to this library. This library does not inherit permissions from its parent Web site*". This therefore means that the users or groups you see listed below are the only users or groups that have rights to this document library as they have been copied from the previous instance when the rights were inherited.

Another point to consider is that because SharePoint now supports security trimming users who do not have explicit rights to this Document Library will not even see it displayed on the *Quick Start* menu. You can also tell the rights are explicit because of the selector boxes at the left of each user or group. These checkboxes allow you to select one or more entries and make changes to these entries via the options in the menu.
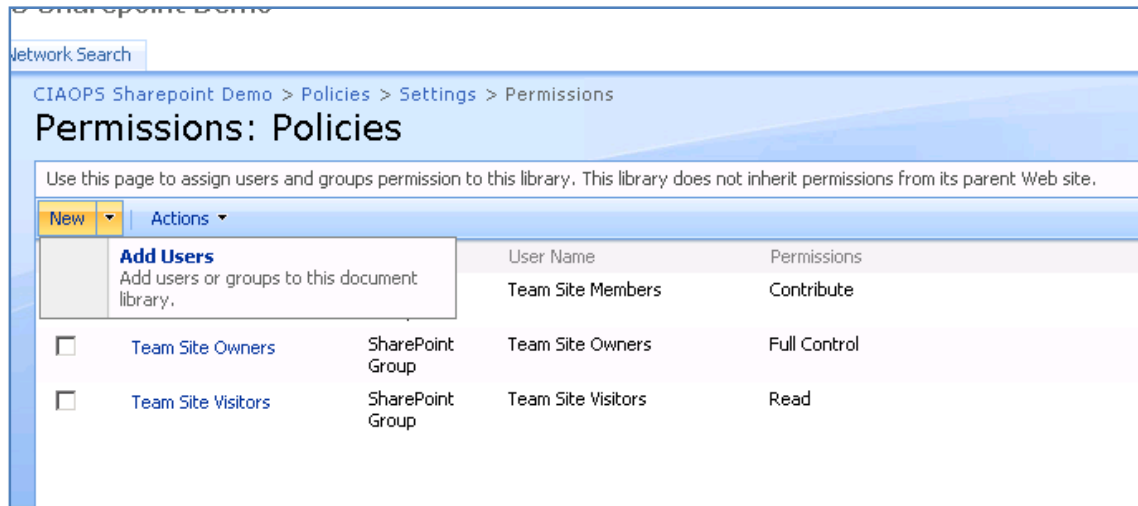
To permit a new user rights to this Document Library now you much select **New** then **Add Users** from the menu bar.

An *Add Users* window will appear. In the section at the top of the screen called *Add Users* enter the names of the users or groups you wish to add. You can check that a user is valid by clicking on the person and checkmark icon at the bottom of the box. You can also use the book icon to look up users already known by the system.

Once you have added the user correctly you should see it underlined.

In the bottom of the window you can now select exactly which rights you wish to give these users. You may firstly choose to add the user to an existing SharePoint group or you may choose to provide them individual rights to the Document Library including:

-   *Full Control*: all rights
-   *Design*: View, add, update, delete, approve and customize.
-   *Contribute*: View, add, update and delete.
-   *Read*: Can view only.

All rights automatically include the rights of the items below them. Thus, the *Contribute* right includes all of the rights associated with *Read* as well as the ability to add, update and delete. You can also only select one of these rights for the user.

When this is complete, press the **OK** button to save the settings.

Any changes to rights take effect immediately although some users may be required to log out and log back into the system for these to completely take effect.
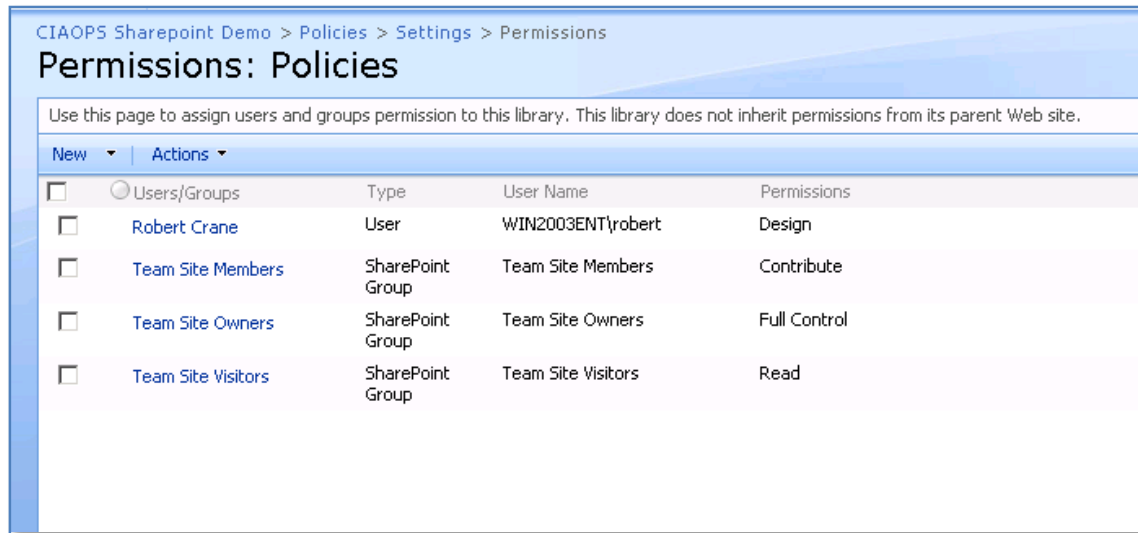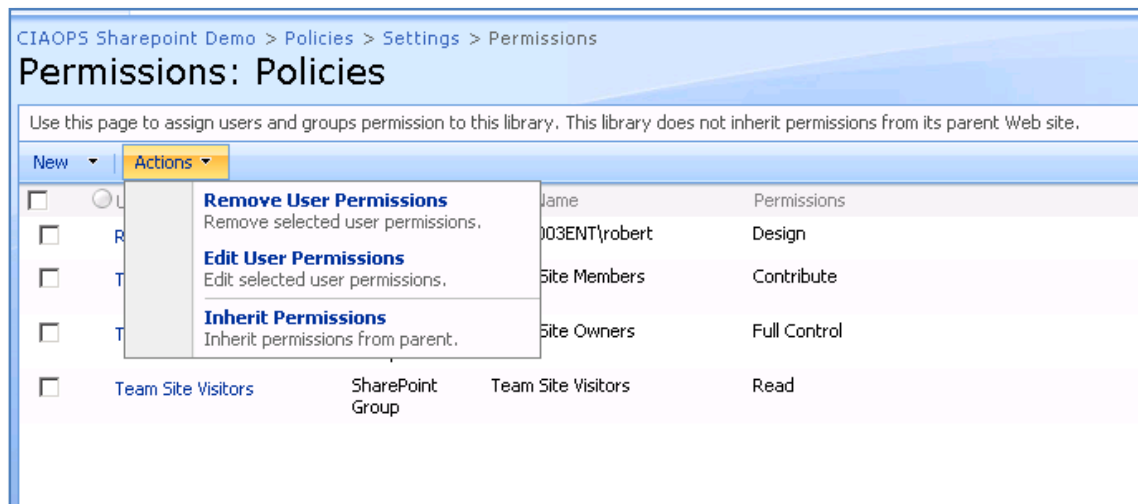

When you are returned to the *Permissions* page you should see the new users in the list with the set of rights that were just assigned (in this case Robert Crane with Design rights at the top of the list).


If you wish to remove users rights from the Document Library simply click in the selector box to the left of their name and from the menu choose **Actions** then **Remove User Permissions**. You will be prompted with a warning before any users are removed.

Likewise, you can edit the rights of any user who already appears in the list by again clicking on the selector box to the left of their name and choosing **Actions** then **Edit User Permissions** from the menu. This will take you back to a window very similar to *Add Users* one shown previously where you can adjust any rights as necessary.

Finally, you can also revert the rights back to where they were inheriting from the parent. To do this simply select **Actions** then **Inherit Permissions** from the menu bar. You will asked to confirm the action and when complete, all the existing rights will be removed and the Document Library will once again inherit the rights from its parent as it did by default.
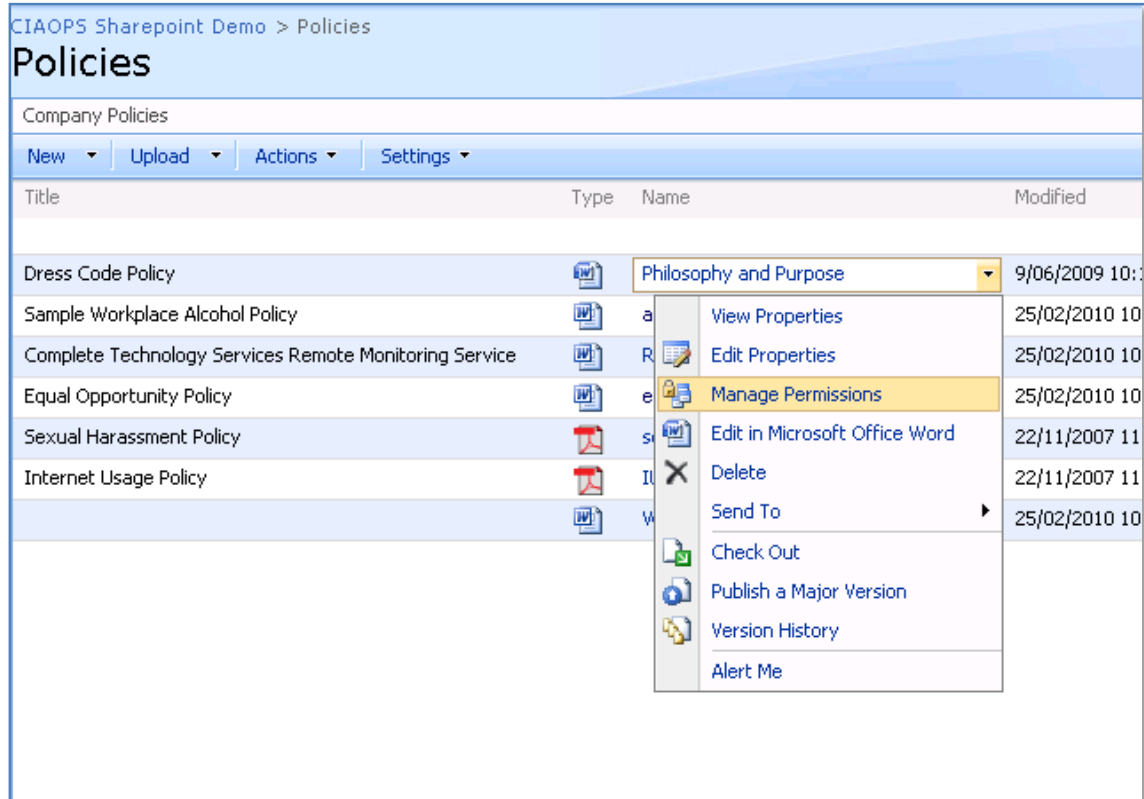
One of the big advantages that WSS v3 brought was the ability to assign rights or permissions for individual items in a Document Library. To do this go to the Document Library where the item you wish to individually secure resides. Select the *properties menu* for that item by selecting the pull down menu at the right of the linked item field as shown above.

From the menu that appears select **Manage Permissions**.

You will then be taken to the Permissions for that item (in this case Philosophy and Purpose). This is very similar to the *Add User* permissions window mentioned previously in that you should firstly see that the item is automatically inheriting its rights from its parent (i.e. the Document Library). You can tell this by what is shown in the informational line displayed just above the menu bar. In this case it reads "*This document inherits permissions from its parent folder or library. To manage permissions directly, click Edit Permissions from the Actions menu*".
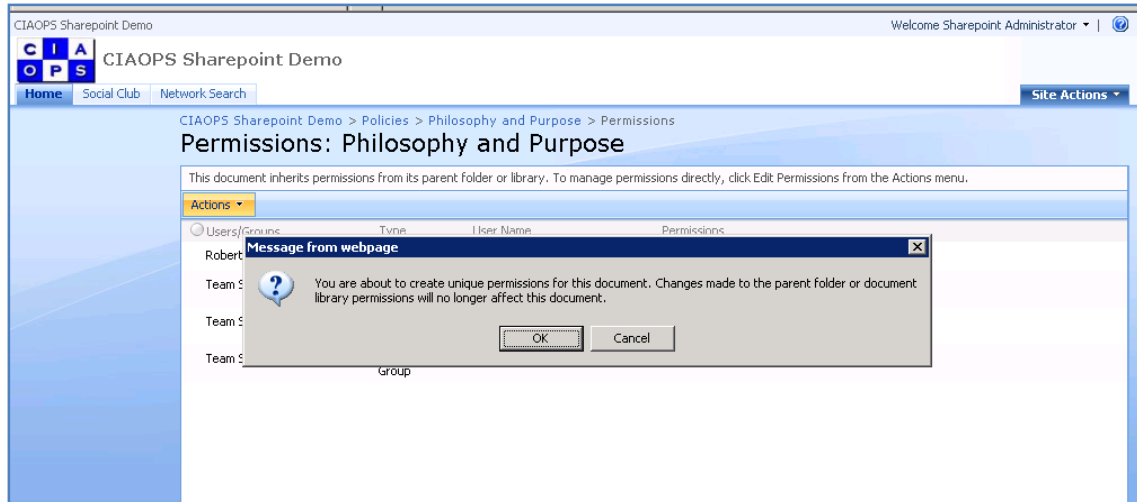
This means that to create unique rights for this document this inheritance needs to be broken.

To break this inheritance select **Actions** then **Edit Permissions** from the menu bar as shown above.

You will be prompted to confirm this action.

Press **OK** to continue.
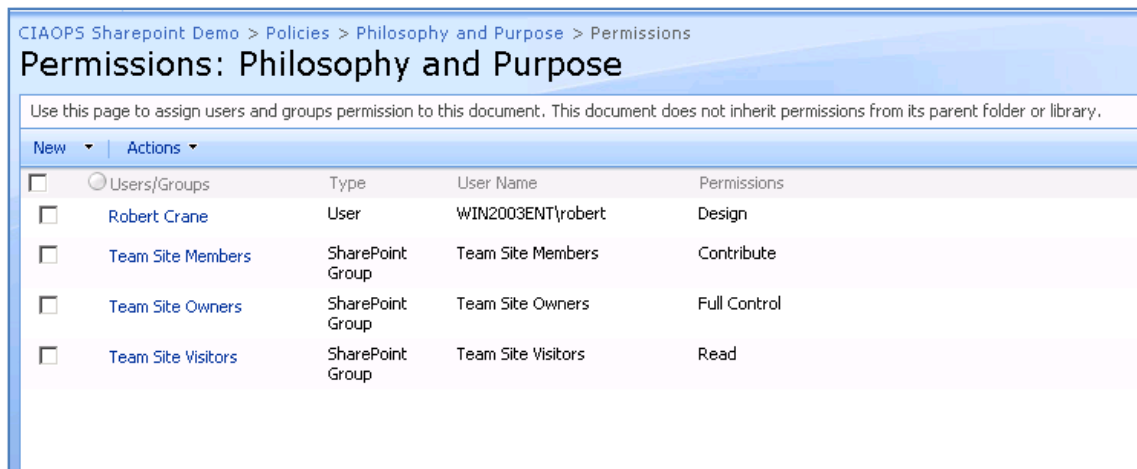
You will then be returned to the *Permissions* window where you will now see selector boxes next to each user. You will also note that the informational line reads – "*Use this page to assign users and groups permissions to this document. This document does not inherit permissions from its parent folder or library*",indicating that permissions for this item are unique.
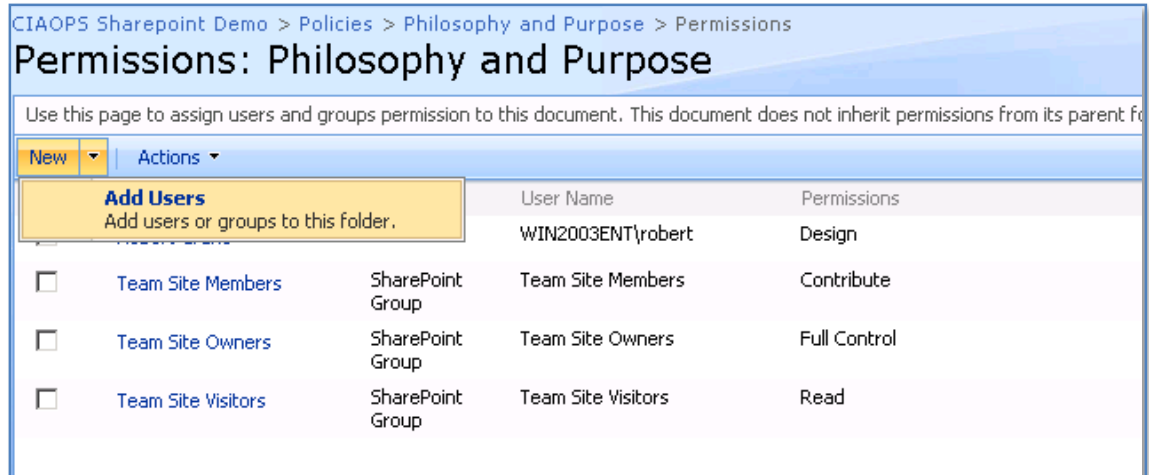
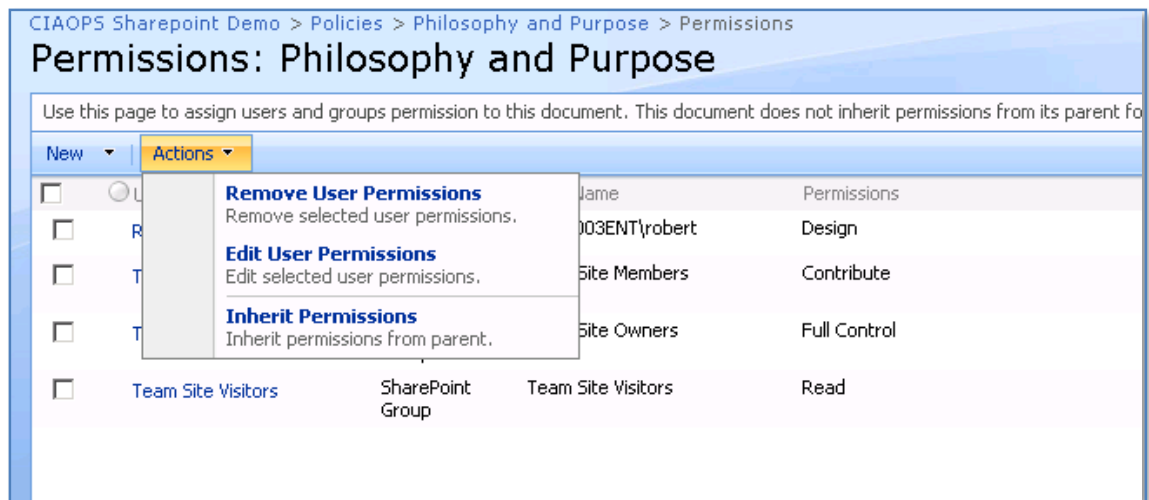As mentioned before, to give users the rights to this item simply select **New** then **Add Users** from the menu bar and assign them the desired rights.

In much the same way as mentioned before, from the *Action* menu you can select to:

- **Remove User Permissions** by selecting the check box to the left of the user and then selecting this option. After a confirmation warning, this user will no longer have any rights to the item.

- **Edit User Permissions** by selecting the check boxes to the left of the user and then selecting this option. You will be taken to the permissions area again where you can make any desired changes.

- **Inherit Permissions**, allowing the item to return to obtaining its rights from its parent (in this case the document library).

Some general points to consider here are that assigning to security rights in SharePoint is a very manual task and needs to be generally done on each element by firstly breaking the default inheritance and then assigning the desired rights. It is therefore best practice to assign rights directly to either Active Directory groups or SharePoint Groups and then add users to these groups. This generally means that the process of assigning rights to individual elements only needs to be done once.

Assigning individual users rights at different locations in SharePoint can make troubleshooting at a later stage time consuming and should be avoided where possible.

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.