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
- 15.2 Security
- 15.3 Default WSF Groups
- 15.4 Adding users to WSF
- 15.7 Enabling anonymous site access
- 15.9 Conclusion

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.

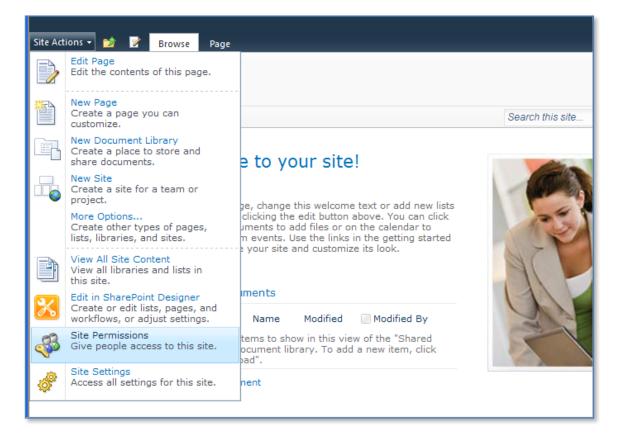
Full Control – a user with these rights has full access to all content and security of the WSF site. They can also create sub-sites.

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.

			Permission Too	ols				
Site Actions 👻 🐋	Brows	ie	Edit					
&, 🐉	8	3	R	R	& ?	🥵 Perm	ission Levels	
Grant Create Permissions Group	Edit (Permis		Remove User Permissions	Check Permissions	Anonymous Access			
Grant		Mo	dify	Check		Manage		
Libraries			Name				Туре	Permission Levels
Site Pages			Anonymo	us Users			Anonymous Users	Entire Web site
Shared Documents	;							
Lists			Team Site	Members			SharePoint Group	Contribute
Calendar			Team Site	Owners			SharePoint Group	Full Control
Tasks			Team Site	Visitors			SharePoint Group	Read
Discussions								
Team Discussion								
🗟 Recycle Bin								
All Site Content	t							

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*.

Site Actions 👻 📩			
	Gite Settings ► People and Groups - grant people contribute permissions to the Sh		5
Home			Search this site
Groups	New - Actions - Settings -		
Team Site Members	Add Users		
Team Site Visitors	Add users to this group.	About Me	Job Title
Team Site Owners	There are no items to show in this view of the	e "User Information List" li	ist.
More			
Libraries			
Site Pages			
Shared Documents			
Lists			
Calendar			
Tasks			
Discussions			

To add users select **New | Add Users** from the menu across.

Grant Permissions		□ ×
Select Users You can enter user names, group names, or e-mail addresses. Separate them with semicolons.	Users/Groups: wfs.ciaops.com\rcrane ;	& 11
	OK Cancel	

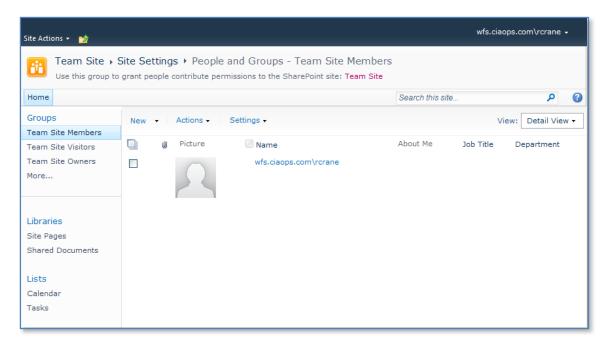
You should now see the above screen. Into the area under *Select Users* you can enter the name of network users or groups. You can enter new users simply by typing their name or network logon. In some cases you may need to use domain/login name. To ensure that WSF can add the specified user press the *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.

Select People an	d Group	os Webpage Di	alog			Đ
http://wfs.ciaops.co	m/_layout	s/Picker.aspx?MultiS	elect=True8	kCustomProperty=I	User%2CSecGrou	up%2CSPGro
Find						Q
Display Name	Title	Department	E-Mail	Mobile Number	Account	Name
Type into the	search bo	x above then press	"Enter" to st	tart your search.		
Add ->						
		_				
			0	DK .	Cance	1
;//wfs.ciaops.com/_la	u au tha (Dia)	key serv2MultiCelectu	-Truce Q.C. ush	emBrenerku-I 🙆	Takayaak	

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.

Select People and Gro	ups	Webpage Di	alog		
http://wfs.ciaops.com/_lay	outs/Pic	ker.aspx?MultiSe	elect=Tru	e&CustomProperty=	User%2CSecGroup%2CSPGroup
Find rcrane					٩
Display Name	Title	Department	E-Mail	Mobile Number	Account Name
wfs.ciaops.com\rcrane					wfs.ciaops.com\rcrane
Add -> wfs.ciaops.com	ı\rcrar	<u>16</u>		OK	Cancel
http://wfs.ciaops.com/_layouts/	Picker.a	spx?MultiSelect=	=True&Cu	stomProperty=L 🍯	Internet

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).

Site Actions 👻 🐋			wfs.ciaops.com\rcrane +
💼 Team Site 🕨	User information: w	rfs.ciaops.com\rcrane - wfs.ciaops.com\rcrane	
Home			
Libraries			Close
Site Pages Shared Documents	Edit Item My Reg	ional Settings My Alerts	
Lists	Account	wfs.ciaops.com\rcrane	
Calendar	Name	wfs.ciaops.com\rcrane	
Tasks	E-Mail		
	Mobile Number		
Discussions	About Me		
Team Discussion	Picture		
	Department		
🔊 Recycle Bin	Job Title		
All Site Content	SIP Address		
		PM by wfs.ciaops.com\administrator 11:54 PM by wfs.ciaops.com\administrator	Close

Once you click on the user you are able to go in and edit their details by selecting **Edit Item** from the menu.

Edit Personal Settings		□ ×
Browse		
	Save Cancel	
🖉 Attach File		
Account	wfs.ciaops.com\rcrane	
Name *	wfs.ciaops.com\rcrane	
E-Mail		=
Mobile Number		
About Me		
Picture	Type the Web address: (Click here to test) http:// Type the description:	
Department		~

Once you have completed editing the information press **OK** to save and continue.

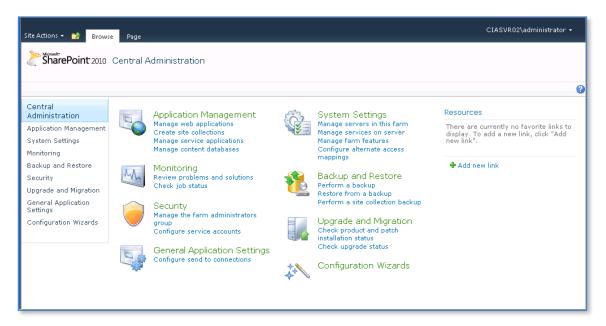
Team Site N			
	Iser information: Rober	rt Crane - wfs.ciaops.com\rcrane	
Home			
Libraries			Close
Site Pages Shared Documents	🗒 Edit Item My Regional	Settings My Alerts	
Lists	Account	wfs.ciaops.com\rcrane	
Calendar	Name	Robert Crane	
Tasks	E-Mail	director@ciaops.com	
	Mobile Number	555-555-5555	
Discussions	About Me		
Team Discussion	Picture		
Recycle Bin		0 2 5	
All Site Content	Department		
	Job Title	Principal	
	SIP Address		

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).

 Internet Explorer (64-bit) Internet Explorer Windows Update Accessories 	
Administrative Tools Maintenance Microsoft SharePoint 2010 Products SharePoint 2010 Central Administration SharePoint 2010 Management Shell SharePoint 2010 Products Configuration Wi	Administrator Documents Computer
Microsoft SQL Server 2008	Network Control Panel Devices and Printers Administrative Tools Help and Support Run
Back	
Search programs and files	Log off

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.

Site Actions 👻 😏 Bro	wse Web Applications				CIASVR02\administrator 👻
	General Settings - Service Connections	Authentication Self-Service Site Providers	Blocked File Types User Permissions Web Part Security	User Anonymous Permission Policy	
Contribute	Manage	Security		Policy	
Central Administration	Name		U	RL.	Port
Application Managemen	t SharePoint - 80		htt	:p://ciasvr02/	80
System Settings	SharePoint Central Administra	ition v4	htt	:p://ciasvr02:37246/	37246
Monitoring					
Backup and Restore					
Security					
Upgrade and Migration					
General Application Settings					
Configuration Wizards					

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

Site Actions 👻 😏 Bro	wse Web Applications				CIA
New Extend Delete	General Settings - Q. Service Connections	Authentication Providers	🌛 Blocked File Types 🐗 User Permissions 👼 Web Part Security	User Anonymous Permission Policy Policy	
Contribute	Manage	Security		Policy	
Central Administration	Name		UF	RL	
Application Managemer	nt SharePoint - 80		htt	tp://ciasvr02/	
System Settings	SharePoint Central Administra	ation v4	htt	tp://ciasvr02:37246/	
Monitoring					
Backup and Restore					
Security					
Upgrade and Migration					
General Application Settings					
Configuration Wizards					

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.

Authenticat	□ ×	
Zone	Mershaushia Duquidau Nama	
Default	Membership Provider Name Windows	

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*).

Edit Authentication		×
Zone These authentication settings are bound to the following zone.	Zone Default	-
Authentication Type Choose the type of authentication you want to use for this zone. Learn about configuring authentication.	Authentication Type © Windows © Forms Click here for details on how to enable Forms Based Authentication in claims mode. © Web single sign on Click here for more details.	
Anonymous Access You can enable anonymous access for sites on this server or disallow anonymous access for all sites. Enabling anonymous access allows site administrators to turn anonymous access on. Disabling anonymous access blocks anonymous users in the web.config file for this zone. Note: If anonymous access is turned off when using Forms authentication mode, Forms aware client applications may fail to authenticate correctly.	► Enable anonymous access	

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.

Internet Information Services (IIS) Manager	
Gerein CIASVR02 → Sites → SharePoint - 80 →	🖬 🖂 🐴 I 🕐 👻
File View Help	
Connections Start Page CIASVR02 (CIASVR02\Administretory Application Pools Sites Default Web Site SharePoint - 80 SharePoint Central Administretory SharePoint Web Services SharePoint Web Services Mindows Authentication Enabled Bises Windows Authentication Enabled Windows Authentication Disabled Windows Authentication Enabled Enabled Bises Windows Authentication Enabled Enabled Bises Windows Authentication Enabled Enabled Bises Windows Authentication Enabled Windows Authentication Enabled Windows Authentication Windows Authentica	Actions Disable Edit @ Help Online Help HT HT
Configuration: 'localhost' applicationHost.config , <location path="SharePoint - 80"></location>	• 1 .:

You will see that Anonymous Authentication at the top of the middle window is *Enabled*.

Site Act	ions 🔻 🐋 📝 🛛 Browse Page			
D	Edit Page Edit the contents of this page.			
	New Page Create a page you can customize.			
Ē	New Document Library Create a place to store and share documents.	e to your site!		
	New Site Create a site for a team or project.	ge, change this welcome text or add new lists to		
	More Options Create other types of pages, lists, libraries, and sites.	king the edit button above. You can click on ents to add files or on the calendar to create new se the links in the getting started section to share ustomize its look.		
	View All Site Content View all libraries and lists in this site.			
	Edit in SharePoint Designer	iments		
<u></u>	Create or edit lists, pages, and workflows, or adjust settings.	Name Modified 🥃 Modified By		
æ	Site Permissions Give people access to this site.	tems to show in this view of the "Shared ocument library. To add a new item, click "New"		
¢	Site Settings Access all settings for this site.	nent		

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.

		Permission Too	ols				
Site Actions 👻 过	Browse	Edit					
&, 🐉	B	R	R	<u></u>	🐗 Permission Lev 💦 Site Collection		
Grant Create Permissions Group	Edit User Permissions	Remove User Permissions	Check Permissions	Anonymous Access			
Grant	M	odify	Check		Manage		
Libraries		🖉 Name				Туре	Permission Levels
Site Pages		Team Site	Members			SharePoint Group	Contribute
Shared Documents		Team Site	Owners			SharePoint Group	Full Control
Lists		Team Site	Visitors			SharePoint Group	Read
Calendar							
Tasks							
Discussions							
Team Discussion							
🗟 Recycle Bin							
🖄 All Site Content	:						

In the ribbon bar across the top select **Anonymous Access**.

Anonymous Access		□ ×
Anonymous Access Specify what parts of your Web site (if any) anonymous users can access. If you select Entire Web site, anonymous users will be able to view all pages in your Web site and view all lists and items which inherit permissions from the Web site. If you select Lists and libraries, anonymous users will be able to view and change items only for those lists and libraries that have enabled permissions for anonymous users.	Anonymous users can access Entire Web site C Lists and libraries Nothing	5:
	OK	Cancel

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 subsites that inherit their permissions from this parent site.

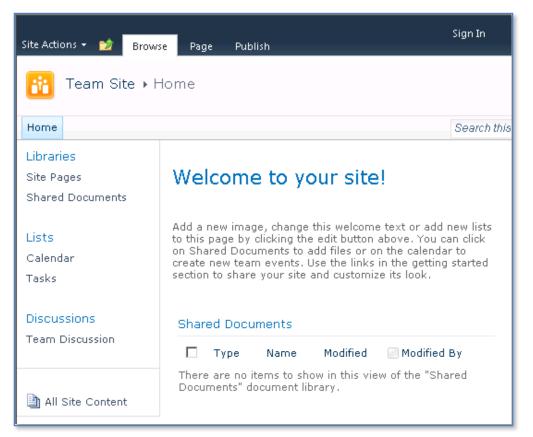
Lists and libraries: any user can access any list or library in any part of the WSS v3 site that has been explicitly enabled for anonymous access. They are unable to navigate by viewing other pages and can only access the list or library via a direct link.

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.

		Permission To	ols -				
Site Actions 👻 対	Browse	Edit					
Grant Create	Edit Us		Check	Anonymous Access	Permission Leve		
Permissions Group Grant	Permissi		Permissions	Access	Managar		
Grant		Modify	Check		Manage		
Libraries	ſ	📃 📃 Name				Туре	Permission Levels
Site Pages		Anonymo	us Users			Anonymous Users	Entire Web site
Shared Documents	; -						
Lists	Γ	Team Site	Members			SharePoint Group	Contribute
Calendar	Γ	Team Site	Owners			SharePoint Group	Full Control
Tasks	Γ	Team Site	Visitors			SharePoint Group	Read
Discussions							
Team Discussion							
All Site Content	t						

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*).

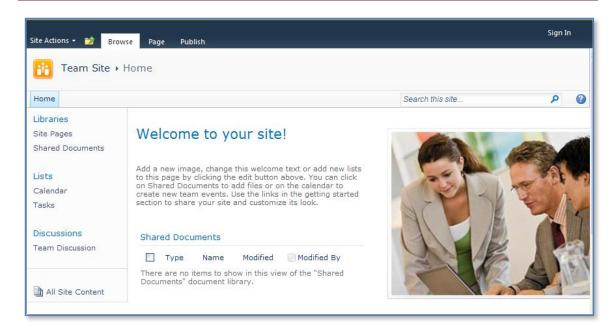
If you click the **Sign In** link you will automatically be logged into WSF as the current network user.



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**.

	Windows Internet Explorer Image: Construction of the second s
×	Sign Out: Close Browser To Complete Sign Out You must close your browser to complete the sign out process.
	€ Go back to site

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.

Site Actions 👻 🔡 Brow		s.ciaops.com\rcrane +
	Tasks → All Tasks → ist to keep track of work that you or your team needs to complete.	
Home	Search this site	۹ (
Libraries Site Pages	Type Title Assigned To Status Priority Due Date % Com There are no items to show in this view of the "Tasks" list. To add a new item, click "New".	pplete Predecessors
Shared Documents	🕈 Add new item	
Lists Calendar		
Tasks		
Discussions Team Discussion		
All Site Content		

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.

Site Actions 👻 😥 Bro	List T wse Items	List			wfs.ciaops.com	n\rcrane +
Standard Datasheet Data	sheet Create View	Current V All Task	s RSS Feed ent Page	Sync to SharePoint Workspace Connect to Outlook Export to Excel Connect & Export	e V IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	List Settings
Libraries Site Pages Shared Documents Lists Calendar Tasks Discussions			Assigned To Sta	tus Priority Due Date ist. To add a new item, click "New		redecessors

Then select list settings from the ribbon bar at the top right of the window.

	Tasks → List Settings			
Home Libraries	List Information		6)	
Site Pages Shared Documents Lists Calendar	Description: Use the Task	http://wfs.ciaops.com/Lists/Tasks/AllItems.aspx Use the Tasks list to keep track of work that you or your team needs to complete.		
Tasks Discussions Team Discussion	General Settings Title, description and navigation Versioning settings Advanced settings Validation settings	Permissions and Management Delete this list Save list as template Permissions for this list Workflow Settings	Communications RSS settings	
Recycle Bin		nultiple content types. Use content types to speci policies, workflows, or other behavior. The follo		

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

Inheritance Check Permissions Inheritance Check his list inherits permissions from its parent. (Team Site) ibraries Name ibraries Anonymous Users hared Documents Team Site Members ists Team Site Owners asks Team Site Visitors		Permission Tools
Inheritance Check his list inherits permissions from its parent. (Team Site) ibraries ibraries ite Pages hared Documents hared Documents Team Site Members ists calendar asks Team Site Owners iscussions eam Discussion Recycle Bin	Site Actions 👻 헌 🛛 Bre	owse Edit
Inheritance Check his list inherits permissions from its parent. (Team Site) ibraries ibraries ite Pages hared Documents hared Documents Team Site Members ists calendar asks Team Site Owners iscussions eam Discussion Recycle Bin	😓 😹	R
his list inherits permissions from its parent. (Team Site) ibraries ibraries ite Pages hared Documents Team Site Members Calendar asks Team Site Owners Team Site Visitors Discussions eam Discussion	Manage Stop Inheriting Parent Permissions	Check Permissions
ibraries ite Pages hared Documents Team Site Members ists calendar asks Team Site Owners Team Site Visitors	Inheritance	Check
ite Pages hared Documents Team Site Members ists calendar asks Team Site Owners Sh Gr Team Site Visitors Sh Gr Gr Sh Calendar B Recycle Bin	This list inherits permi	ssions from its parent. <u>(</u>
hared Documents Use ists Team Site Members Sha Gro Team Site Owners Sha asks Team Site Owners Sha iscussions Gro Sha iscussions Gro Gro	Libraries	Name
hared Documents Team Site Members Shar Grou Calendar asks Team Site Owners Team Site Owners Team Site Visitors Calendar	Site Pages	Anonymous Use
ists Grou Calendar Team Site Owners Shar asks Team Site Visitors Shar iscussions Grou Grou Participation Recycle Bin Grou	Shared Documents	
alendar Grou asks Team Site Visitors Shan Discussions Grou Grou	Lists	Team Site Membe
eam Discussion	Calendar	Team Site Owner
eam Discussion	Tasks	Team Site Visitors
	Discussions	
	Team Discussion	
All Site Content	A Recycle Bin	
	🗎 All Site Content	

By default, the list will normally inherit its permissions from the parent site. To prevent this select **Stop Inheriting Permission** from the ribbon bar.

	Pern	nission Tools	wfs.ciaops.com\rcrane +
Site Actions 👻 対 Br	owse	Edit	
🍇 🍪	R		
Manage Stop Inheriting Parent Permissions	Check Permissions		
Inheritance	Check		
This list inherits permi			
Libraries	Messa	ige from wel	opage 🔼
Site Pages	?) You are at	out to create unique permissions for this list. Changes made to the parent site permissions will no longer affect this list.
Shared Documents	- T		
			OK Cancel
Lists			
Calendar	Team	Site Owners	SharePoint Full Control Group
Tasks	Team	Site Visitors	SharePoint Read Group
Discussions			
Team Discussion			
A Recycle Bin			
All Site Content			

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

Permission Tools Site Actions - Drowse Edit					
Inherit Permissions	Edit User Permissions	Check Permissions	Anonymous Access		
Inheritance Grant	Modify	Check	Manage		
This list has unique permissions					
Libraries	Name			Туре	Permission Levels
Site Pages Shared Documents	Anonymous U	sers		Anonymous Users	View Items
Lists	Team Site Mer	nbers		SharePoint Group	Contribute
Calendar	Team Site Own	ners		SharePoint Group	Full Control
Tasks	Team Site Visi	tors		SharePoint Group	Read
Discussions					
Team Discussion					
Recycle Bin					

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.

Anonymous Access	□ ×
Anonymous Access Specify what permissions anonymous users have in this list.	 Anonymous users can: Add Items - Add items to lists. Edit Items - Edit items in lists. Delete Items - Delete items in lists. View Items - View items in lists, documents in ✓ document libraries, view Web discussion comments, and set up alerts for lists.
	OK Cancel

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 <u>director@ciaops.com</u>.