



SharePoint 2013 Permissions Guide

Author: Brett Lonsdale

Company: Lightning Tools

Date: 7th July 2015

Twitter: www.twitter.com/lightningtools

Facebook: www.facebook.com/lightningtools

Web: www.lightningtools.com

Introduction

Microsoft SharePoint puts a lot of responsibility into the hands of the SharePoint Site Owner or Site Collection Administrator. The key thing to understand about Site Owners and Site Collection Administrators is that they are not typically SharePoint Farm Administrators, and usually have very little education about managing the sites that they own. Permission inheritance is often broken when it shouldn't be, Limited Access is often misunderstood, Users are not removed from SharePoint groups when they leave the organization, and when to use Active Directory Groups vs SharePoint Groups is not well understood either.

The purpose of this document is to provide a guide as to how permissions work in SharePoint 2013 and can also be applied to SharePoint Online. If you use SharePoint 2010, you will find an equivalent guide here: http://lightningtools.com/sharepoint_2010/sharepoint-2010-permissions-management-guide/

Within this guide, we will explore the following topics:

- SharePoint Permissions Overview
- Securable Objects
- Assigning Permissions
- Sharing Content
- Permission Levels
- New Edit Permission
- Permission Inheritance
- Managing Permissions with DeliverPoint

SharePoint Permissions Overview

SharePoint Permissions can be assigned to user accounts directly, via Active Directory Groups or by the user becoming a member of a SharePoint Group. It is also possible for permissions to be granted

LightningTools

to users by an Active Directory group being nested in a SharePoint Group. A new user interface feature of SharePoint 2013 is the 'Share' button which can also be used to grant permissions to users.

The below figure shows the User/Domain Groups can be added to SharePoint Groups or assigned a permission level directly. SharePoint Groups are mapped to a permissions level which determines the permissions that the user/group receives.

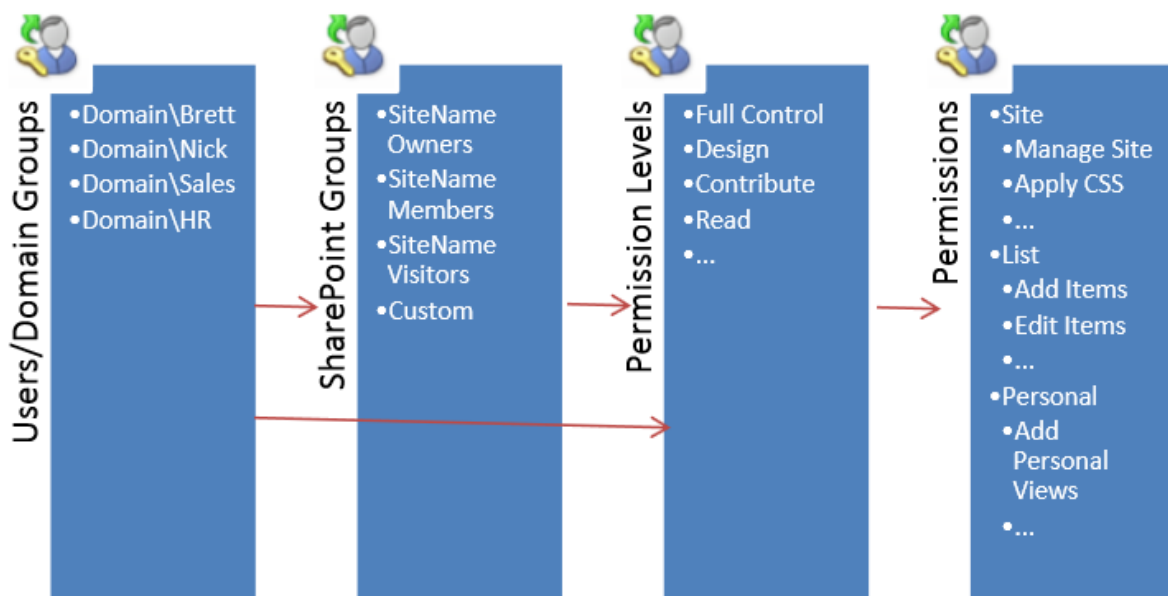


Figure 1 – Assignment of Permissions

Securable Objects

Within each SharePoint site collection, there are securable objects. Each site contains an Access Control List (ACL) of which contains the associations between user/group and permissions. Each site contains lists which also have an ACL. Folders and Items within each list, again have an ACL. The permissions by default inherit the ACL from the parent object. E.g. A subsite inherits from the parent site. A list or a library inherits from its containing site, and each folder or item inherits from the list or parent folder. The inheritance can be broken at any point so that unique permissions can be assigned. E.g. you may grant Edit permissions to a Document store in a library for Fred, when Fred only had Read permissions to the Site.

A typical site collection could look like the diagram below whereby there is a mixture of sites and other objects that either inherit their permissions or they have unique permissions.

LightningTools

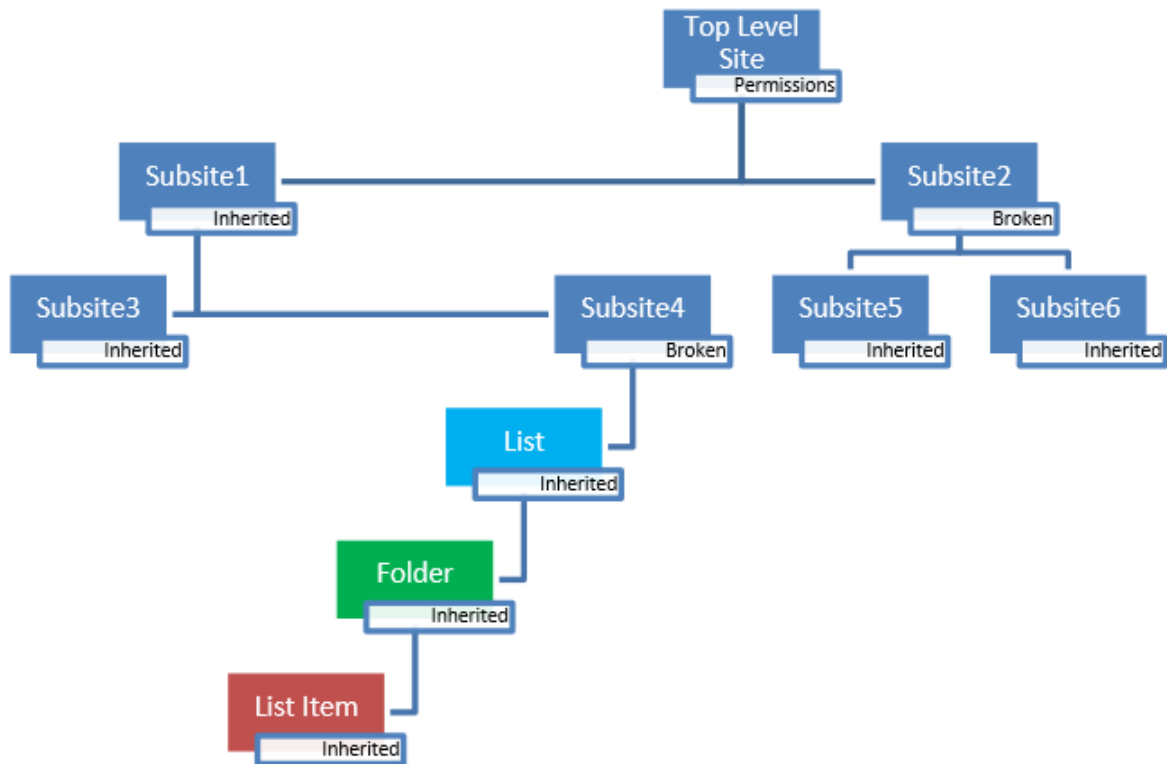


Figure 2 – Site Collection showing securable objects.

Assigning Permissions

Permissions can be assigned using multiple methods and each method has its own advantages and disadvantages.

- Directly assign permissions to a user. E.g. Fred received Contribute permissions
- Assign permissions to an Active Directory Group. Add a user to the relevant AD group.
- Add a user to a SharePoint Group that is already assigned a permission level.
- Add an Active Directory Group to a SharePoint Group.
- Click Share on a Site, List, Folder, or Item and share the content with a specific user.

One of the issues with the SharePoint permissions reporting is that it will not enumerate the Active Directory Groups. Therefore, the permission report displays the direct permissions only for the individual user, Active Directory Group or SharePoint Group. If a user had received permissions from an Active Directory Group, you may not be aware of it.

LightningTools

If you consider a newly created site setup with the following:

SharePoint Group	User/Active Directory Group	Permission Level
'Permissions Guide Visitors'	DP\Students	Read
'Permissions Guide Members'	DP\Sales	Edit
'Permissions Guide Owners'	DP\Brett	Full Control

Assigning permissions via an Active Directory Group

The DP\Students and DP\Sales Active Directory Groups both contain many users. The SharePoint Permissions Report displays as per below. You can see the SharePoint Groups permission levels.

Name	Type	Permission Levels
<input type="checkbox"/> <input type="checkbox"/> Permissions Guide Members	SharePoint Group	Edit
<input type="checkbox"/> <input type="checkbox"/> Permissions Guide Owners	SharePoint Group	Full Control
<input type="checkbox"/> <input type="checkbox"/> Permissions Guide Visitors	SharePoint Group	Read
<input type="checkbox"/> <input type="checkbox"/> System Account	User	Full Control

Figure 3 Permissions Report on a Site

Upon clicking the link for a SharePoint Group, you will see the members of that group, but will not see the members of an Active Directory Group.

Name	Members
<input type="checkbox"/> DP\sales	

Figure 4 you cannot see who is a member of the DP\Sales group

LightningTools

If you are fully aware as to who the members of the Active Directory are, this will not concern you. Using Active Directory groups to assign permissions, means that should a user leave the organization or transfer to another department, you have a single place to remove them.

Assigning Permissions via a SharePoint Group

SharePoint Groups provide a very easy way for Site Owners and Site Collection Administrators to manage SharePoint permissions. When you provision a new Team Site with Unique Permissions, you will have the option to create three new SharePoint Groups; *Site_Name_Visitors*, *Site_Name_Members* and *Site_Name_Owners*. The groups are mapped to Read, Edit and Full Control respectively. Therefore, to assign a user the user 'Edit' permission level, you can simply add the user to the relevant group.

It is also possible to create additional SharePoint Groups. For example, you may create a SharePoint group to represent each department or project within your organization. Although it is worth keeping in mind that the SharePoint Groups are scoped to the Site Collection.

To Create a SharePoint Group in SharePoint 2013:

1. Navigate to **Site Settings** by clicking the cog in the top right hand corner.
2. Under **Users and Permissions** click **People and groups**
3. Click the **Groups** heading so that all Groups are displayed.
4. Click **New, New Group**.

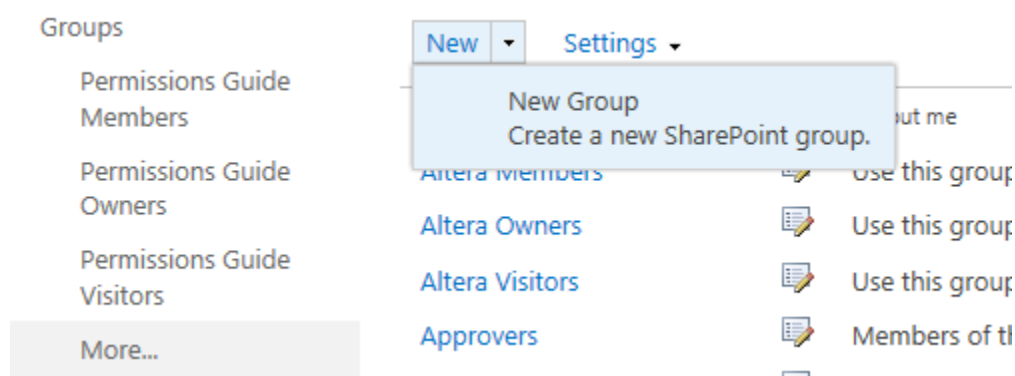


Figure 5 creating a new group

Name and About Me

Provide a **Name** for your group, and a description for the group in the **About Me** column.

Owner

The Group Owner will default to the currently logged on user. A consideration is the subsequent fields that depending on the configuration could mean that only the Group Owner can modify the membership of the group. This could be an issue if the Group Owner were to leave the organization



or the account is deleted. You cannot add a Domain Group to the Group Owner field, but it is possible to add a SharePoint Group. It may therefore be a good idea to add the *sitename_owners* group as the group owners if this is applicable. You can also only add a single user account as the owner.

Group Settings

Within the Group Settings you can specify who can view the membership of the group. The default is Group Members, but you can make the list available to everyone.

You can set Group Owner or Group Members to be able to edit the membership of the group. The default is Group Owner.

Membership Requests

The Membership Requests options are useful for joining SharePoint Discussion Lists or Community Sites where security may not be a concern. i.e. you can sign up to use a discussion list. You can therefore make requests to join a group which upon approval would make you a member and assign a permission level to you. It is possible to have any request automatically accepted.

Give Group Permission to this Site

As mentioned previously, a group is scoped to the site collection. It can therefore be assigned different permission levels to different sites, lists, folders and items. For example, you could create a 'Sales' SharePoint Group, assign it Full Control to the Sales Team Site, but assign the same group Read permission level to the Marketing Team Site. This option allows you to specify the permission level that the group will be assigned to this specific site.

LightningTools

SharePoint

Name and About Me Description
Type a name and description for the group.

Name:

About Me:

Rich text editor toolbar and text area.

Owner
The owner can change anything about the group such as adding and removing members or deleting the group. Only one user or group can be the owner.

Group owner:

Group Settings
Specify who has permission to see the list of group members and who has permission to add and remove members from the group.

Who can view the membership of the group?
 Group Members Everyone

Who can edit the membership of the group?
 Group Owner Group Members

Membership Requests
Specify whether to allow users to request membership in this group and allow users to request to leave the group. All requests will be sent to the e-mail address specified. If auto-accept is enabled, users will automatically be added or removed when they make a request.

Allow requests to join/leave this group?
 Yes No

Auto-accept requests?
 Yes No

Send membership requests to the following e-mail address:

Give Group Permission to this Site
Specify the permission level that you want members of this SharePoint group to have on this site. If you do not want to give group members access to this site, ensure that all checkboxes are unselected.

Choose the permission level group members get on this site: <http://intranet.dp.local/sites/esp14/permissions/permguide>

- Full Control - Has full control.
- Design - Can view, add, update, delete, approve, and customize.
- Edit - Can add, edit and delete lists; can view, add, update and delete list items and documents.
- Contribute - Can view, add, update, and delete list items and documents.
- Read - Can view pages and list items and download documents.
- View Only - Can view pages, list items, and documents. Document types with server-side file handlers can be viewed in the browser but not download.
- Approve - Can edit and approve pages, list items, and documents.

Figure 6 – Creating a SharePoint Group.

SharePoint Groups vs Active Directory Groups

If you intend to share SharePoint content using groups, you will typically have the choice of Active Directory Groups or SharePoint Groups.

Your company may have a preference here of 'Only use SharePoint Groups' or 'Only use Active Directory Groups'. That of course should be honoured as a corporate decision.

There are only really two considerations when it comes to using Active Directory groups. Active Directory Groups are not just there for SharePoint. They have typically be designed around the organization structure of the business and group membership has an impact on other networked resources such as CRM, SQL permissions, File Share permissions and also Distribution groups used for email purposes. Therefore, SharePoint users cannot simply add/remove users to groups, instead a request should be made. The other consideration is that the groups are not enumerated within SharePoint. Users therefore cannot see a list of group members, and therefore calculate who has permissions to their content.

SharePoint Groups overcome both of these considerations. SharePoint Groups can be managed by users, and allow for the enumeration of its members. However, they are only scoped to the Site Collection which can cause issues when trying to apply permissions to content that is contained in different site collections.

LightningTools



Below is a diagram comparing both types of groups:

SharePoint Groups	Active Directory Groups
Maintained by Users within SharePoint	Should Reflect the organizational structure
Easily view membership	Scope (Beyond a single site collection)
Users can Add/Remove Members	Single point of removal for retiring employee
Membership Requests	Managed by Domain Admins
Can be managed by the SharePoint Object Model	Difficult to work out permissions for users in AD groups

Assigning Permissions Directly to Users

Assigning permissions directly to users is possible, but that shouldn't mean that you should ☺ If you assign permissions directly to a user, there could be hundreds or thousands of folders, list items and documents whereby permissions have been assigned directly. Consider what would happen if that user was to leave the organization. Using SharePoint out-of-the-box would mean literally iterating through thousands of objects looking to see if a permission has been assigned on a given object. Powershell could be used to remove the permissions, but what if another user should receive them instead?

Assigning permissions via a SharePoint Group or Active Directory group is a preferred method so that there is a single point of removal.

To assign permissions directly:

1. Choose **Site Actions, Site Settings**.
2. Click **permissions** from under the Users and Permissions category.
3. Click Grant Permissions.
4. Enter the name of the person that you would like to share with. (Notice that the default permission level is Edit).
5. Click More Options to apply a different permission level.
6. The Permission Levels and the SharePoint Groups are mixed together in the (Select a Group or Permission Level) drop down.

LightningTools

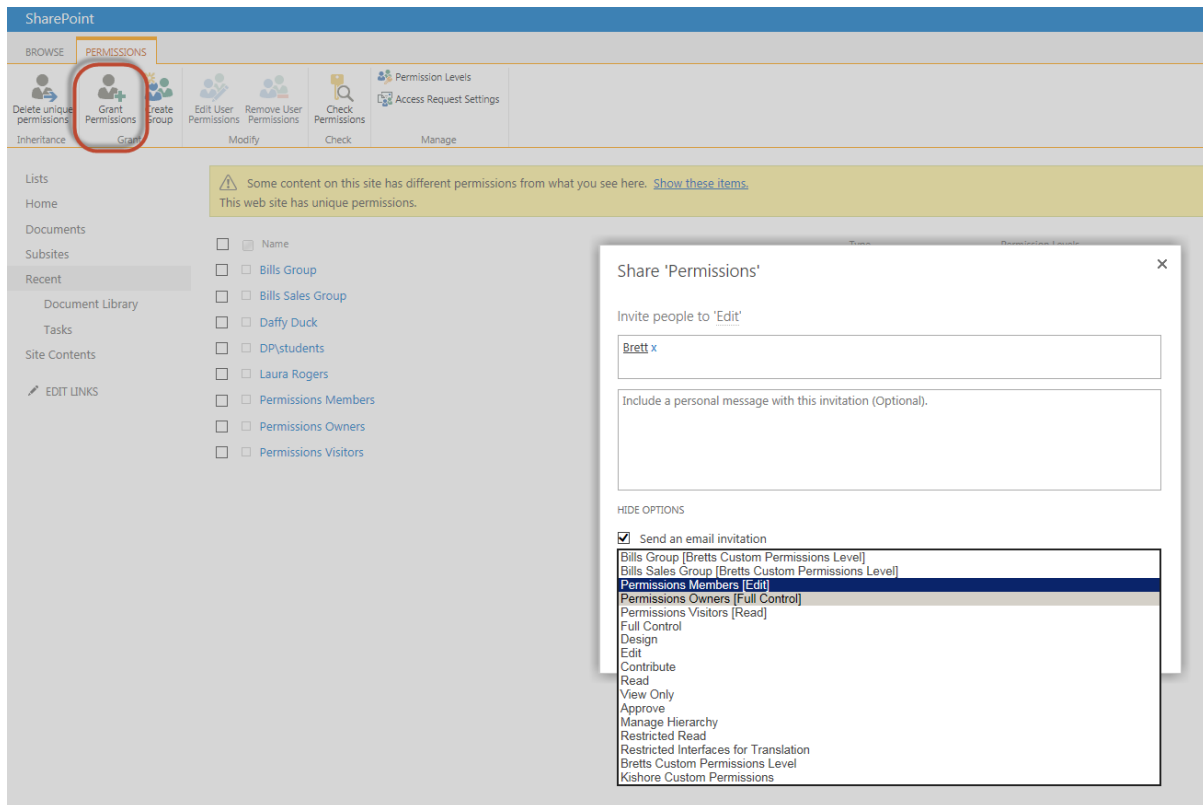


Figure 7 – Granting Direct Permissions to a user

7. Select from **Full Control, Design, Edit, Contribute, Read, View Only, Manage Hierarchy, or Restricted Read**. Custom Permission levels may display also.

In order to assign permissions to lists, libraries, folders or items, the same method can be applied although you may need to break the permission inheritance first. (See Permission Inheritance).

Share option

SharePoint 2013 also provides a 'Share' option which invites users to share content by assigning permissions.

Any object can be shared by anyone, although sharing will require approval by an Admin user if you do not have the 'Manage Permissions' role on the object that you are sharing.

Depending on what you share, and how you share it, will affect whether permission inheritance is broken on the object that you are sharing. This can cause broken permission inheritance to be common within SharePoint lists and libraries.

LightningTools

[Share Site \(web\)](#)

If you Share a site by clicking the 'Share' option in the top right hand corner of a site, the default will be that users to invite will receive 'Edit' permissions. 'Edit' is a powerful permission level enabling users to manage and delete lists, so this should be discouraged.

If you accept the default 'Edit', Invitees will become a member of the Members group either with the site or where the site inherits its permissions from. Therefore, great care must be taken, since you are potentially granting Edit permissions to your intended site, but also to its parent site and content.

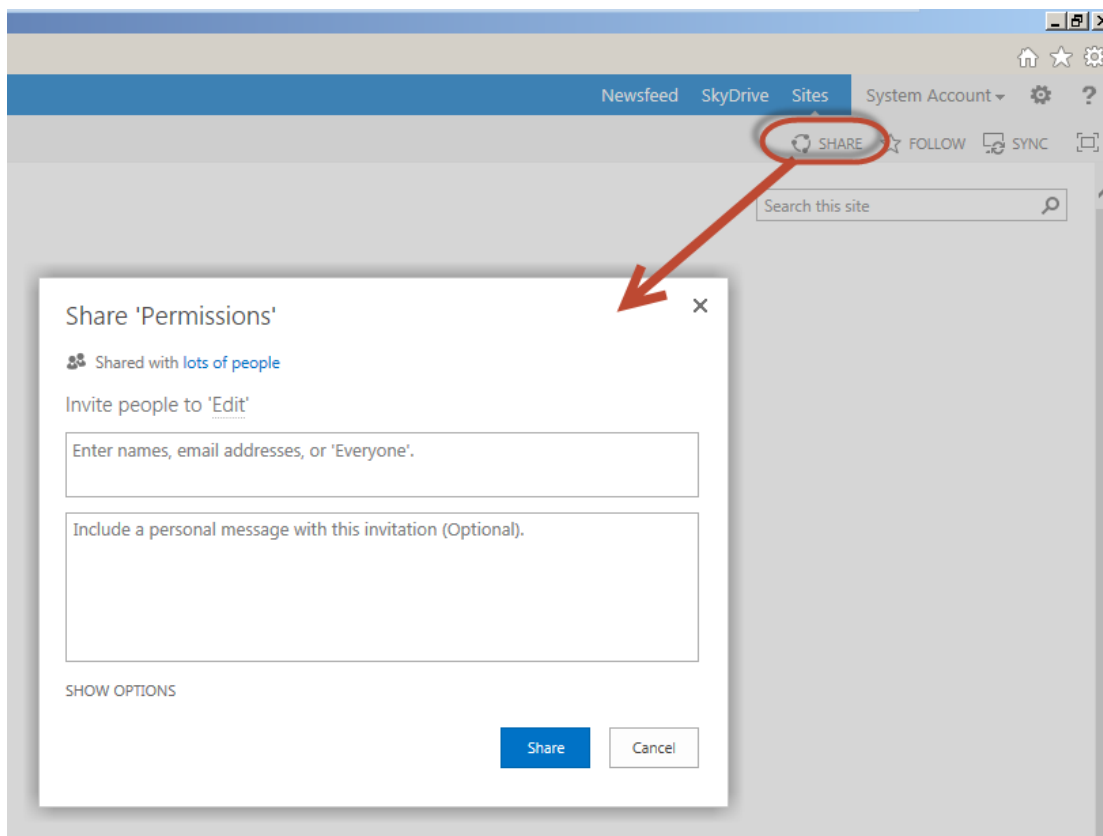


Figure 8 – Share Permissions at Site Level.

Note, that when you Share a site, permission inheritance for that site is not broken.

Of course, you can click the Show Options link to change from Edit to another SharePoint Group or permission level other than Edit.

[Sharing a List/Library](#)

Sharing a list or a library can be done from the list/library ribbon. Firstly, click 'Shared With' and then 'Invite People. This time, Permission Inheritance **WILL BE BROKEN**. Any invitees will receive direct

LightningTools

permissions to the List/Library. This could cause big problems since the library would no longer inherit permissions from the parent site object as was originally intended.

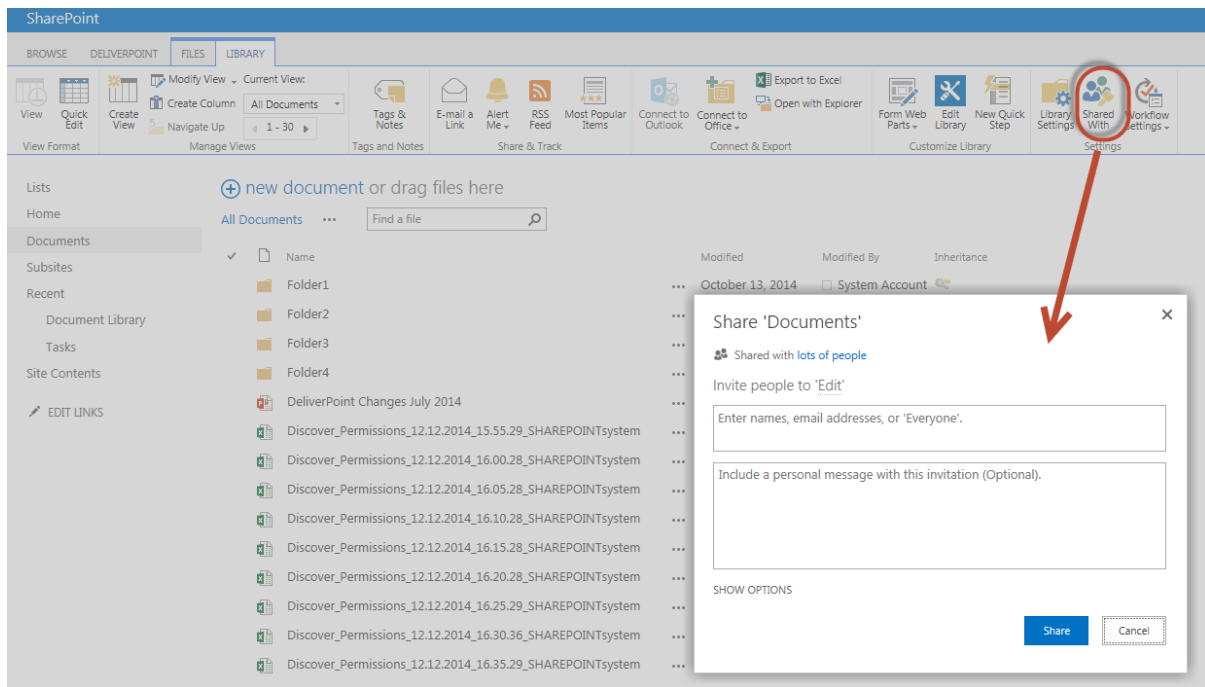


Figure 9 – Share Permissions at List level

Sharing Folders

Sharing Folders via the ellipsis will default to 'Can Edit'. The invitee won't actually receive 'Edit' permissions though, they will receive 'Contribute' permissions to the folder. The folder inheritance will also be broken, and the users permissions assigned directly. 'Can View' is another option via the drop down which would provide the user with Read permission level.

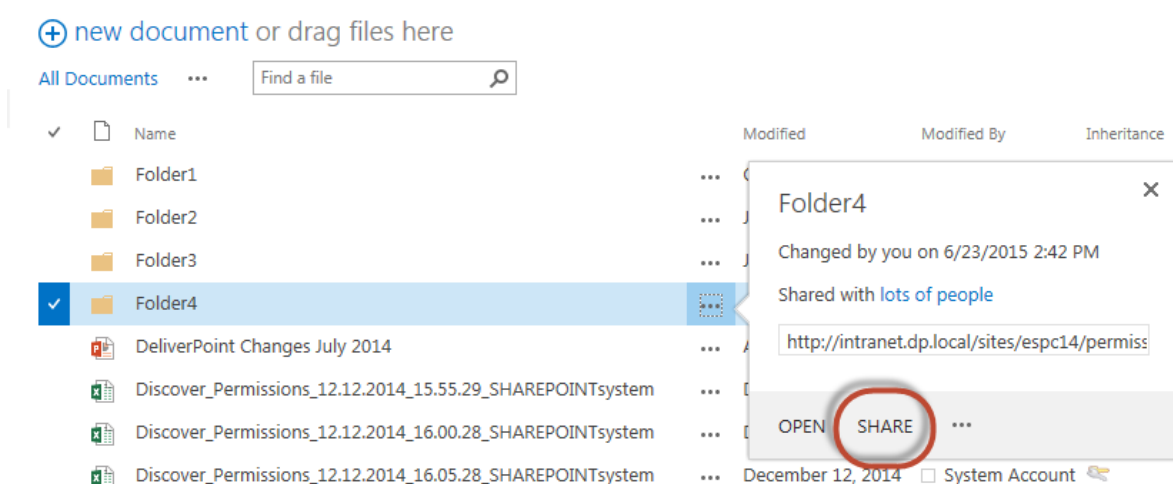




Figure 10 – Share Permissions at Item/Folder level.

Sharing Documents

Clicking the Share option under the Document or List item ellipsis will result in the document permission inheritance being broken. Any users are given Contribute (Can Edit) or Read (Can View) permissions.

Permission Levels

The SharePoint permission levels vary depending on the CAL that you are using with SharePoint 2013. SharePoint Foundations for example has fewer permission levels since it has less functionality.

Permission Levels in SharePoint 2013 are made up of 3 different categories of permissions; Site, List and Personal permissions. There are 18 individual site permissions, 12 List permissions, and 3 personal permissions. Therefore, organizing these individual permissions into permission levels, makes it a much simpler process to assign permissions to groups and individuals.

SharePoint Foundations contains the following permissions:

- Full Control
- Design
- Edit
- Contribute
- Read
- Limited Access

Edit is a new SharePoint 2013 Permission level which has become the permission level assigned to the Members group. In SharePoint 2010 and prior, the default permission level assigned to Members was Contribute. If you migrate from SharePoint 2010 to 2013, the 2010 members groups will be upgraded but will continue to be assigned the Contribute permission level.

The following tables have been copied from support.office.com (Understanding Permission Levels)

Site Permissions

Permission	Full Control	Design	Edit	Contribute	Read	Limited Access
Manage Permissions	X					
View Web Analytics Data	X					
Create Subsites	X					
Manage Web Site	X					
Add and Customize Pages	X	X				
Apply Themes and Borders	X	X				
Apply Style Sheets	X	X				
Create Groups	X					



Browse Directories	X	X	X	X		
Use Self-Service Site Creation	X	X	X	X	X	
View Pages	X	X	X	X	X	
Enumerate Permissions	X					
Browse User Information	X	X	X	X	X	X
Manage Alerts	X					
Use Remote Interfaces	X	X	X	X	X	X
Use Client Integration Features	X	X	X	X	X	X
Open	X	X	X	X	X	X
Edit Personal User Information	X	X	X	X		

List Permissions

Permission	Full Control	Design	Edit	Contribute	Read	Limited Access
Manage Lists	X	X	X			
Override List Behaviors	X	X				
Add Items	X	X	X	X		
Edit Items	X	X	X	X		
Delete Items	X	X	X	X		
View Items	X	X	X	X	X	
Approve Items	X	X				
Open Items	X	X	X	X	X	
View Versions	X	X	X	X	X	
Delete Versions	X	X	X	X		
Create Alerts	X	X	X	X	X	
View Application Pages	X	X	X	X	X	X

Personal Permissions

Permission	Full Control	Design	Edit	Contribute	Read	Limited Access
Manage Personal Views	X	X	X	X		
Add/Remove Private Web Parts	X	X	X	X		
Update Personal Web Parts	X	X	X	X		

Limited Access

Limited Access is assigned to an individual automatically by SharePoint, when the user in question has been granted permissions directly to an object with broken permission inheritance. For example, Assume a user called Brett has No Access to a SharePoint Team Site. However, Permission Inheritance is broken on a list within the SharePoint Team Site, and Brett is granted the Edit permission level on the list. Brett will therefore automatically be assigned Limited Access to the SharePoint Team Site.

LightningTools

Edit

Edit is a new permission level in SharePoint 2013 which is very similar to Contribute permission level with the exception that users can Manage lists. Edit therefore allows users to Add Site Columns and manipulate lists a lot more. Unfortunately, it also means that the list can be deleted by a user with Edit permissions, so it should therefore be used with caution.

Creating a Custom SharePoint Permission Level

You should not alter the existing permission levels within SharePoint although it is possible at the top level site within the Site Collection. Instead, you should consider creating a custom permission level. Custom Permission Levels can be created within SharePoint allowing you to specify exactly the permissions that you require within your own level. For example, you may require a permission level similar to that of Contribute, but without the ability to delete content. To create a custom permission level:

1. Navigate to the Top Level **Site Settings**.
2. Click **Site Permissions**
3. Click Permission Levels under **Manage**.

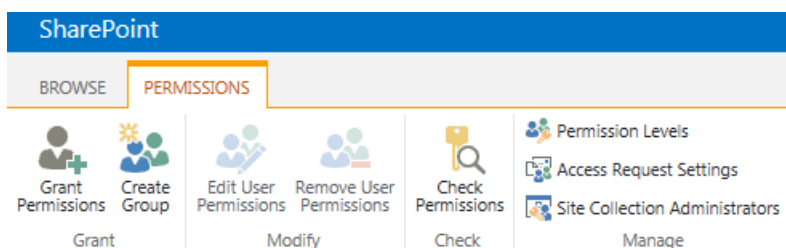


Figure 11 – Add a permission Level

4. Click an existing permission level rather than clicking **Add a Permission Level**.
5. Scroll to the bottom of the Permission Level page, and click **Copy Permission Level**.
6. Provide a **name** and a **description** for your custom permission level.
7. Remove or add additional permissions.
8. Click **Create**.

You can now assign users to your custom permission level directly or by assigning a SharePoint Group to the permission level.

Permission Inheritance

Permission Inheritance can be broken at any level. The default when you create new sub sites, lists/libraries, folders, list items/documents, is that they inherit the permissions from their parent. If you wish to make a change to the permissions on an object that is inheriting permissions, you must first break permission inheritance. This includes adding new users or groups as well as removing them.

LightningTools

By navigating to the SharePoint Permissions page of any object, you will notice the 'Stop Inheriting Permissions' button on the Permissions ribbon.

Clicking Stop Inheriting Permissions will break the permission inheritance, but will also allow you to re-inherit permissions should you need to.

The screenshot shows the SharePoint interface. At the top, there is a blue header with the text 'SharePoint'. Below this is a ribbon with two tabs: 'BROWSE' and 'PERMISSIONS'. The 'PERMISSIONS' tab is active. Under the 'PERMISSIONS' tab, there are three buttons: 'Manage Parent' (with a group icon), 'Stop Inheriting Permissions' (with a group icon and a red 'X'), and 'Check Permissions' (with a magnifying glass icon). Below the ribbon, there are two sections: 'Inheritance' and 'Check'. The 'Inheritance' section shows a yellow banner with a warning icon and the text 'This list inherits permissions from its parent. (Permissions)'. The 'Check' section shows a list of permissions with checkboxes: Name, Bills Group, Bills Sales Group, Daffy Duck, DP\students, Laura Rogers, Permissions Members, Permissions Owners, and Permissions Visitors. On the left side of the page, there is a navigation pane with links for Lists, Home, Documents, Subsites, Recent, Announcements, Inherit, Document Library, Tasks, Site Contents, and EDIT LINKS.

Figure 12 – Breaking Permission Inheritance

The yellow banner on the permissions page will explain to you whether the object is inheriting permissions from its parent, or whether it has unique permissions.

Permission Inheritance should be broken only if it is absolutely necessary. Remember also, that sharing a folder or list item will also result in broken SharePoint permission inheritance.

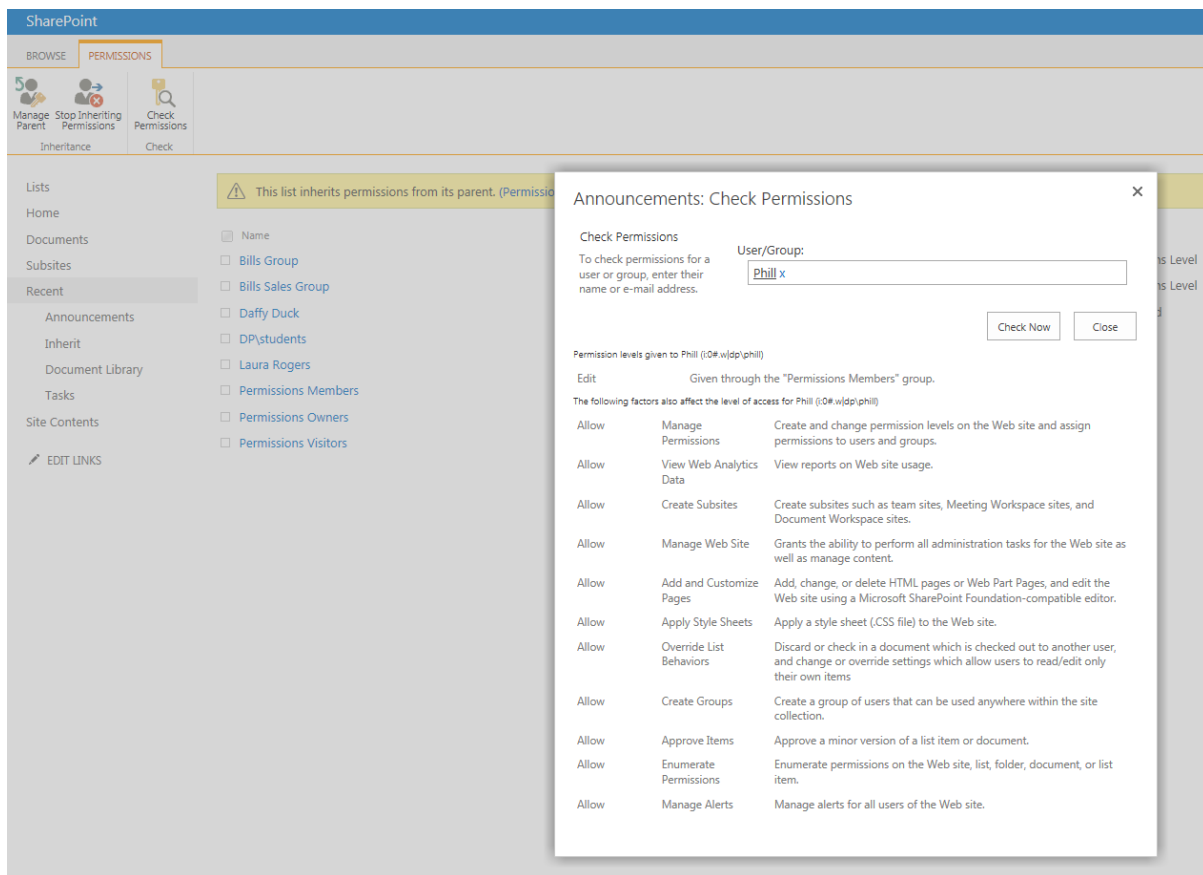
Check Permissions

Ever since SharePoint 2010, Microsoft SharePoint has a 'Check Permissions' option. This is a useful tool to check what permissions a user has. If you suspect that an individual has been granted permissions via an Active Directory group, you could click the Check Permissions button to determine their permissions even if that user does not show in the standard permission report.

LightningTools

Take for example 'Phill' in the below permission report. He is not shown as having direct permissions and is only permitted via the Active Directory Group 'Sales' which is nested in the Permission Members group.

Check Permissions confirms that the user does in fact have permissions.



The screenshot shows the SharePoint interface with the 'PERMISSIONS' tab selected. A modal dialog titled 'Announcements: Check Permissions' is open. The dialog contains a 'User/Group' field with 'Phill x' entered and 'Check Now' and 'Close' buttons. Below the input field, it lists the permission levels given to the user and the factors affecting their access.

Permission levels given to Phill (i:0#.w dp phill)	
Edit	Given through the "Permissions Members" group.

The following factors also affect the level of access for Phill (i:0#.w|dp|phill)

Level	Permission	Description
Allow	Manage Permissions	Create and change permission levels on the Web site and assign permissions to users and groups.
Allow	View Web Analytics Data	View reports on Web site usage.
Allow	Create Subsites	Create subsites such as team sites, Meeting Workspace sites, and Document Workspace sites.
Allow	Manage Web Site	Grants the ability to perform all administration tasks for the Web site as well as manage content.
Allow	Add and Customize Pages	Add, change, or delete HTML pages or Web Part Pages, and edit the Web site using a Microsoft SharePoint Foundation-compatible editor.
Allow	Apply Style Sheets	Apply a style sheet (.CSS file) to the Web site.
Allow	Override List Behaviors	Discard or check in a document which is checked out to another user, and change or override settings which allow users to read/edit only their own items
Allow	Create Groups	Create a group of users that can be used anywhere within the site collection.
Allow	Approve Items	Approve a minor version of a list item or document.
Allow	Enumerate Permissions	Enumerate permissions on the Web site, list, folder, document, or list item.
Allow	Manage Alerts	Manage alerts for all users of the Web site.

Figure 14 – Check Permissions

How does Lightning Tools DeliverPoint help with permission reporting and permission management?

DeliverPoint is a Permissions Management tool which is available for SharePoint Online, SharePoint 2007, SharePoint 2010, and SharePoint 2013 even if you are using SharePoint Foundations. DeliverPoint provides better reporting and management features so that Site Owners, Site Collection Administrators and SharePoint Admins can better manage SharePoint permissions within their environments.

LightningTools

Permission Inheritance

Using DeliverPoint, you can see clearly which objects have inherited versus unique permissions. The below screenshot shows a Document Library and you can see clearly the documents with unique permissions with the full colour inheritance icon.

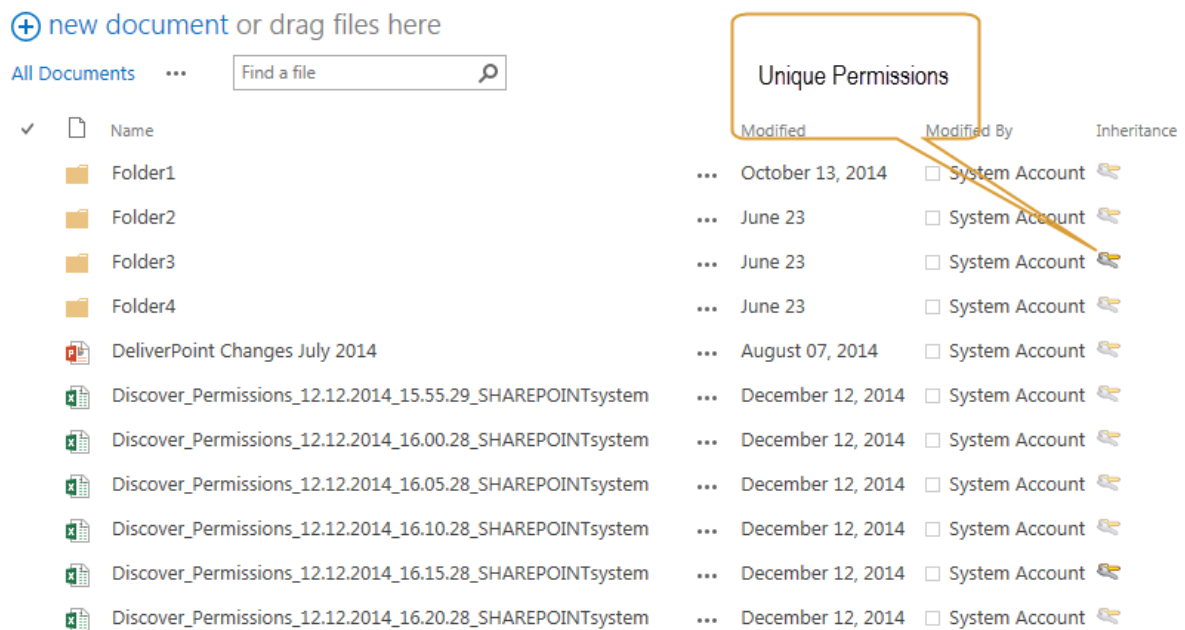


Figure 15 – DeliverPoint Inheritance Icon within a Library.

Sites and lists also show as full colour icons if permission inheritance is broken within the DeliverPoint treeview:

LightningTools

The screenshot displays the LightningTools interface for SharePoint. On the left, a TreeView shows a hierarchy of sites under 'Server Farm'. A yellow callout bubble points to a site icon with a full color, stating 'Full Colour means broken permission inheritance'. The right pane shows navigation instructions and a Treeview Legend.

Full Colour means broken permission inheritance

Using the View Tab

Account Centric:	Search for account permissions
Farm Centric:	View your SharePoint Site hierarchy
Treeview Legend:	Defines the symbols used in the Treeview
Job Status and History:	View your pending and completed jobs

Using the Treeview

+/- allows you to drill down through the SharePoint Site hierarchy

Select a node to view action available for the scope

Treeview Legend

- Farm
- Web Application
- Managed Path
- Site Collection
- Site - Inherits Permissions: This site inherits permissions from its parent.
- Site - Unique Permissions: This site defines its own permissions.
- Site - No Access: The current user does not have access to this site.
- Site - Unknown Access: The current user does not have access to view another user's permissions on this site.

Last Interrogation: 06 JUL at 09:14PM

Figure 16 – DeliverPoint TreeView showing inherited sites

Active Directory Group Enumeration

If a user has been assigned permissions via Active Directory Groups, the users permissions are still shown in the DeliverPoint permission reports:

LightningTools

The screenshot shows the SharePoint interface with the 'PERMISSIONS' ribbon selected. The 'Permissions' section is expanded, displaying a list of users and their assigned permissions. The 'Permissions' column shows 'Full Control (Implicit)' for most users, while some have 'Edit' permissions. A red box highlights the 'Permissions Members' group, which includes 'DP.developers' and 'Dmitry'.

Site	User Name	Permissions	Permissioned Via
Site	administrator	Full Control (Implicit)	Site Collection Administrators
	Ardee Rivera	Full Control (Implicit)	Site Collection Administrators
	bill	Full Control (Implicit)	Site Collection Administrators
	Julia	Full Control (Implicit)	Site Collection Administrators
	Zoe	Full Control (Implicit)	Site Collection Administrators
	Ardee Rivera	Full Control	Permissions Owners
	John Ross	Full Control	Permissions Owners
	Laura Rogers	Full Control	Permissions Owners
	Julia	Full Control	Permissions Owners
	System Account	Full Control	Permissions Owners
	bill	Edit	Permissions Members
	Brett	Edit	Permissions Members
	Daffy Duck	Edit	Permissions Members
	Phill	Edit	Permissions Members
	Dmitry	Edit	Permissions Members
	Michael	Edit	Permissions Members
	John Ross	Edit	Permissions Members

Figure 16 – Permission Report showing how permissions were assigned.

Unique Permission Reports

The Unique Permission report can be run from the Server Farm, Web Application, Site Collection and Site scopes. The report shows all Account members including Active Directory Groups, as well as Site Permissions, List Permissions and List Item permissions.

The screenshot shows the 'REPORT' ribbon in SharePoint, with the 'Unique Permissions' report selected. The report displays a list of permissions for the 'esp14' site collection. The 'Account' column lists various groups and users, and the 'Permission Level' column shows the assigned permissions. The report is filtered by the 'esp14' site collection.

Account	Site Collection	Site	Permission Level
Permissions Visitors	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14	Design
Petromash Members	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14	Design
Roadshow Permissions Members	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14	Design
Rowan Members	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14	Design
Sales Team Site Members	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14	Design
Seaboard Members	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14	Design
SharePoint Days Permissions Members	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14	Design
TV Sales Members	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14	Design
Style Resource Readers	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14	Design
Brett	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14	Design
Brett	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14/SAP	Design
Brett	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14/SLAC	Design
Brett	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14/social	Design
Brett	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14/test123	Design
DP.Sales	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14/permissions/Allera	Full Control
DP.Sales	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14/permissions/deliverpointtraining	Full Control
DP.Sales	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14/permissions/di-data	Full Control
Altera Members	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14/permissions/Altera	Edit
Bills Group	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14/permissions	Bretts Custom Permissions Level
Bills Group	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14/Rowan	Bretts Custom Permissions Level
Bills Group	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14/SAP	Bretts Custom Permissions Level
Bills Group	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14/SLAC	Bretts Custom Permissions Level
DeliverPoint Training Members	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14/permissions/deliverpointtraining	Edit
DiData Members	http://intranet.dp.local/sites/esp14	http://intranet.dp.local/sites/esp14/permissions/di-data	Edit

Figure 17 – Unique Permissions Report

LightningTools

Permission Operations

Permission Operations can be performed in bulk on multiple objects at a time. Including:

- Copy Permissions
- Transfer Permissions
- Delete Permissions
- Grant Permissions
- Clone Permissions

Take for an example, that a user is leaving the organization, but is being replaced by a new member. Permissions can therefore be transferred from the old user to the new user within a single operations covering all objects within a given scope.

Audit Permissions

If permissions change, you may want to know about it. DeliverPoint allows you to monitor permission changes that are performed using SharePoint out of the box, using PowerShell or using DeliverPoint.

SharePoint						
BROWSE		COMMANDS				
Permission Management						
Show Changes After		Show Changes Until				
Permission Changes						
Date	Initiator	Scope	Changed Via	Permission	Member	
<input type="checkbox"/> 7/3/2015 12:40:59 PM	SHAREPOINT\system	TEST123	TEST123	Design		dpl/zoe
<input type="checkbox"/> 7/3/2015 12:40:59 PM	SHAREPOINT\system	TEST123	TEST123	Full Control		dpl/zoe
<input type="checkbox"/> 7/3/2015 12:40:59 PM	SHAREPOINT\system	TEST123	TEST123	Full Control		dpl/laura
<input type="checkbox"/> 7/3/2015 12:40:59 PM	SHAREPOINT\system	TEST123	TEST123	Design		dpl/daffyduck
<input type="checkbox"/> 7/3/2015 12:40:59 PM	SHAREPOINT\system	TEST123	TEST123	Approve		Approvers
<input type="checkbox"/> 7/3/2015 12:40:59 PM	SHAREPOINT\system	TEST123	TEST123	Manage Hierarchy		Hierarchy Managers
<input type="checkbox"/> 7/3/2015 12:40:59 PM	SHAREPOINT\system	TEST123	TEST123	Restricted Interfaces for Translation		Translation Managers
<input type="checkbox"/> 7/3/2015 12:40:59 PM	SHAREPOINT\system	TEST123	TEST123	Restricted Read		Restricted Readers
<input type="checkbox"/> 7/3/2015 12:40:58 PM	SHAREPOINT\system	TEST123	TEST123	Read		ESPC14 Visitors
<input type="checkbox"/> 7/3/2015 12:40:58 PM	SHAREPOINT\system	TEST123	TEST123	Edit		ESPC14 Members
<input type="checkbox"/> 7/3/2015 12:40:58 PM	SHAREPOINT\system	TEST123	TEST123	Design		Designers
<input type="checkbox"/> 7/3/2015 12:40:58 PM	SHAREPOINT\system	TEST123	TEST123	Design		dpl/brett
<input type="checkbox"/> 7/3/2015 12:40:58 PM	SHAREPOINT\system	TEST123	TEST123	View Only		Excel Services Viewers
<input type="checkbox"/> 7/3/2015 12:40:58 PM	SHAREPOINT\system	TEST123	TEST123	Full Control		ESPC14 Owners
<input type="checkbox"/> 7/3/2015 12:31:00 PM	SHAREPOINT\system	SLAC	SLAC	Design		dpl/zoe
<input type="checkbox"/> 7/3/2015 12:31:00 PM	SHAREPOINT\system	Social	Social	Design		dpl/zoe
<input type="checkbox"/> 7/3/2015 12:31:00 PM	SHAREPOINT\system	London Office	Social	Design		dpl/zoe
<input type="checkbox"/> 7/3/2015 12:31:00 PM	SHAREPOINT\system	Technical Support	Social	Design		dpl/zoe
Permission Inheritance Changes						
Date	Initiator	Scope	Changed Via			
<input type="checkbox"/> 7/3/2015 12:35:49 PM	SHAREPOINT\system	TEST123	TEST123			
Groups Members Changes						
Date	Initiator	Site	Group	User		
<input type="checkbox"/> 7/6/2015 2:32:40 PM	SHAREPOINT\system	espc14	Permissions Members		dpl/michael	
<input type="checkbox"/> 7/6/2015 2:32:19 PM	SHAREPOINT\system	espc14	Permissions Members		dpl/michael	

Figure 18 – Auditing Permissions with DeliverPoint

LightningTools

Permission Alerts

If permission changes are business critical, DeliverPoint will notify you. Simply configure an alert. If permission inheritance is broken, or if a user is granted permissions to an object, you can be notified immediately via email.

Compare Permissions

Permissions can be compared between multiple sites/lists or libraries. It is often difficult trying to work out the differences between permissions on different objects. DeliverPoint can produce a comparison report allowing you to compare up to 20 sites at a time.

Operation: Web permissions comparison report. Scope: Permissions, Rollup, Rowan

Webs	Permissions	Rollup	Rowan
User	Limited Access	-	-
dp/landy	Full Control	Full Control	Full Control
dp/ardee	Full Control	Limited Access	Full Control
dp/bill	Limited Access	Edit	Bretts Custom Permissions Level
dp/brett	Bretts Custom Permissions Level	Limited Access	Bretts Custom Permissions Level
dp/chris	Limited Access	-	-
dp/daffyduck	Full Control	Design	Full Control
	Design	Limited Access	Design
	Read	Limited Access	Read
dp/dimtry	-	Limited Access	-
DP/students	Edit	-	Edit
	Read	-	Read
	Limited Access	-	-
dp/julia	Limited Access	Edit	Bretts Custom Permissions Level
	Limited Access	Limited Access	-

Figure 19 – Comparing Permissions across multiple sites with DeliverPoint

I hope that you found this article useful.

Download a free trial of DeliverPoint: <http://lightningtools.com/products/deliverpoint-2013/>

<Lightning Tools/>