

DeliverPoint 2013 and Add-In

1 — Last update: 2017/08/22

Lightning Tools

Table of Contents

DeliverPoint	3
DeliverPoint 2013	4
Deploying DeliverPoint 2013	8
Performance Testing Scenarios	14
Installation Steps	15
Install the DeliverPoint binaries	16
DeliverPoint Configuration Wizard	21
Commence Full crawl of Active Directory and SharePoint.....	27
Check the DeliverPoint installation	34
Activating your DeliverPoint License.....	38
How to find the DeliverPoint version	42
DeliverPoint Checker	43
DeliverPoint Central Administration.....	48
Restricting access to DeliverPoint	60
Powershell Commands	63
Permission Management.....	71
Security Trimming.....	74
DeliverPoint Settings options	76
DeliverPoint dashboard.....	78
Farm Centric view	82
Account Centric view	84
Tree view legend	85
Job Status and History.....	86
Job Details page.....	89
Transaction Types.....	91
Common Commands	92
Discover Permissions	93
Discover Permissions results page.....	97
Refining Discover Permissions results.....	101
Tracking Permission Changes	106
Alerts	108
Auditing.....	114
Permission Inheritance	117
Properties.....	121
Account Management	126
Copy Permissions.....	127

Grant Permissions	132
Transfer Permissions	136
Delete Permissions	140
Revoke Permissions	143
Dead Account Detection	145
Unique Permissions	147
Site Management	149
Compare Site Permissions	150
Copy Site Permissions	152
Unique Lists Detection	157
List Management	159
Copy List Permissions	161
Unique List Items Detection	166
DeliverPoint Inheritance Field	168
Item Permissions	172
Troubleshooting	173
Missing: DeliverPoint Timer Jobs	174
Missing: Manage Lightning Tools Product Licensing link	175
DeliverPoint SharePoint Online Add-In for Office 365	176
Installation and Configuration of the DeliverPoint Add-In	177
Upload Add-In to App Catalog	178
Create Windows Azure Application	179
Adding the Add-In to a Site	187
Configure DeliverPoint Add-In	189
How to tell the version of the Add-In	191
Removing the Add-In from a site	192
Using the Add-in	195
Add-in Tree View Legend	198
Discover permissions using the add-in	199
Discover Permissions add-in report	203
Refining Discover Permissions add-in results	205
DeliverPoint SharePoint Online Add-In for Office 365 Professional	206
Installation and Configuration of the DeliverPoint Add-In	207
Upload Add-In to App Catalog	208
Create Windows Azure Application	209
Adding the Add-In to a Site	220
Configure DeliverPoint Add-In	222
How to tell the version of the Add-In	224

Removing the Add-In from a Site	225
Using the Add-in Professional	228
Add-In ProTree View Legend	232
Discovering Permissions	233
Discover Site and List Permissions	234
Discover Folder, Item, or File Permissions	238
Discover Permissions Results	239
Refining Discover Permissions Results	241
Other Reports	244
Unique Permissions Report (Account Centric View)	245
Compare Permissions Report	248
Managing Permissions	251
Copy Permissions	252
Grant Permissions	256
Transfer Permissions	259
Delete Permissions	262
Permissions Inheritance	265
Inherit or Break Permissions	266

DeliverPoint

[Lightning Tools](#) provides a permissions reporting and management tool for the on-premises installation of [Microsoft® SharePoint®](#), and a permissions reporting SharePoint add-in within your [Office 365™](#) tenant.

Documentation for the different versions of the tool can be found by clicking on the following links:

- [DeliverPoint 2010](#)
- [DeliverPoint 2013/2016](#)
- [DeliverPoint add-in](#)

DeliverPoint 2013

[DeliverPoint 2013](#) is an in-context Microsoft® SharePoint® [Permissions Management](#) Tool that enables SharePoint farm administrators, site collection administrators and site owners to effectively manage SharePoint permissions within the context of a SharePoint on-premises environment.

This page contains links to two recorded webcasts, the [benefits](#) of using DeliverPoint 2013 and an overview of the key [features](#). To learn how to deploy, use or troubleshoot DeliverPoint 2013, click on the following links:

- [Deploying DeliverPoint 2013](#)
- [Permission Management](#)
- [Troubleshooting DeliverPoint 2013](#)

For a brief overview of the product view the following recorded webcast (8:13):

For a deep dive into using DeliverPoint, view the following recorded webcast (50:21):

Benefits

- Provides [permissions management](#) to the business user.
- Provides confidence.
- Cleans up the permissions *mess*.
- Support for Microsoft® SharePoint® 2007, 2010, 2013.

DeliverPoint Features

- Discover where user or group accounts have [unique permissions](#) throughout your farm down to the list item level.
- [Schedule discovery reports](#)
- Specify:
 - A DeliverPoint [operator](#) to manage permissions on any site regardless of their permissions to a SharePoint object
 - [A Permission Auditor](#)
- Discover who in your farm has permissions on any given securable object.
- [Discover](#) lists throughout your farm with unique permissions and use the [DeliverPoint Inheritance Field](#) to display a permission inheritance indicator in list / library views.
- Discover list items with [unique permissions](#).

- [Copy](#) / [transfer](#) / [delete](#) a user, Active Directory group or SharePoint Group's permissions.
- [Grant](#) user or group permissions.
- [Reassign](#) one user group with another user group.
- [Monitor farm growth](#) – limited to DeliverPoint permissions operators & site collection administrators.
- Identify and remove [dead accounts](#) within your farm.
- Clone [site](#) and [list](#) permissions.
- [Compare](#) site permissions.
- [Email](#) a person with permission change information or produce [audit reports](#).

These operations can be executed at the following levels:

- Farm
- Web Application
- Managed path
- Site collection
- Individual site (web)
- List / Library
- Folder / List Item / File

The operations you choose affect all permissions for the targeted account resource in scope. For example, let's say you select "Copy Permissions" at the Managed Path level. Since all site collections within the Managed Path are part of the inheritance chain, they are said to be in scope. Site collections that exist under different Managed Paths would not be in scope because they are not part of the first Managed Path's inheritance chain. It is important to know which objects are in scope for every operation you execute using DeliverPoint. For example, if you select to "Delete Permissions" at the Farm level, then all Web Applications, Managed Paths, site collections, sites (webs), lists, list items and folders are in scope for this action. Be sure to target the execution of permissions at the intended level of inheritance so you don't change permissions for a user on the wrong or unintended objects.



Note DeliverPoint is security trimmed so that those using it can only see information and perform DeliverPoint operations within their native scope of authority that is defined within SharePoint. That being said, it is still important to be certain of the desired scope in which to perform an operation so that unwanted changes do not occur. The Copy, Delete, and Transfer Permissions operations are effective on the following objects:

- * Farm
- * Web Application
- * Managed paths
- * Site collections
- * Sites (webs)

- * Lists
- * List items and folders

The Copy, Delete, and Transfer Permission actions can use Active Directory user or group accounts along with Forms Based Authenticated users and Claims Based Authenticated users. You cannot copy a SharePoint group's permissions. Instead, you can copy any account within a SharePoint group to any other account, whether it's in a SharePoint group or not. In addition, DeliverPoint 2013 gives you introductory statistics on your farm, allowing you to understand the aggregate total, age and size of web applications, managed paths, site collections, webs, and lists within your farm. Using DeliverPoint 2013, you can objectively define the following terms as they relate to the aforementioned objects:

- Small
- Medium
- Large
- New
- Aging
- Old

These terms can then be used to segment your farm, web application, managed path, site collection, or web's statistical information. For example, you can define that a "large" list is a list that has over 200 MB of information or that a list that is older than 105 days is "aging". Once defined, DeliverPoint tells you how many "large" and "aging" lists you have at any scope within your farm. You can view size and aging information for any object as previously described.

[Deploying DeliverPoint 2013 >>](#)

Deploying DeliverPoint 2013

This section provides an overview of the installation and upgrading of DeliverPoint 2013 for Microsoft® SharePoint® 2013. It is essential to read this section of the online documentation and complete the steps in the [Installation Steps](#) section, before you can use DeliverPoint. Information on using and administering DeliverPoint can be found later in the documentation.

To successfully deploy DeliverPoint within your organization, you will need to complete the following steps:

- Plan the use of DeliverPoint within your organisation.
- [Plan the installation of DeliverPoint.](#)
- [Install DeliverPoint](#)

If you have any questions related to this documentation or the DeliverPoint product, please contact Lightning Tools by clicking [Submit Support Ticket](#) on the [Lightning Tools](#) web site.

Installation Planning

LightningTools provides an installation wizard to install DeliverPoint binaries, and a configuration wizard to configure DeliverPoint. You will then need to complete some post configuration tasks before you can fully use DeliverPoint. During this process you will require access to:

- An instance of [Microsoft® SQL Server®](#)
- Your [Microsoft® SharePoint® farm](#).
- Active Directory®.



In a production environment you will need to raise a change request to install DeliverPoint.

Database server

[DeliverPoint 2013](#) uses [Microsoft® SQL Server®](#) as the repository for both [Active Directory®](#) and SharePoint® permission information, retrieved using the two DeliverPoint interrogation [SharePoint® timer jobs](#). DeliverPoint supports [Microsoft® SQL Server®](#) 2005, 2008, 2008 R2, and 2012. Using any other database platform such as Oracle® or SAP® is NOT supported.

The main reason for using an SQL Server database, is performance and scalability. DeliverPoint stores object information in a database rather than work with your SharePoint production databases in real-time so as to increase performance of the application. In larger farms, real-time interrogation of the farm in order to commit an individual administrative action could be too costly in terms of I/O activity, memory, and processor utilization on the SharePoint servers.

The DeliverPoint database holds minimal information about the user, such as account login name and display name, but it does not store account passwords. Hence, from a security perspective, there is no need to encrypt the database, nor should the existence of the account information in the DeliverPoint database be viewed as a security vulnerability since the DeliverPoint database cannot be used for logon purposes. Some of the SharePoint databases contain the same information, for example, the UserInfo table in the SharePoint content database or the SharePoint profile database associated with a User Profile service application. Having another database contain a copy of the same information does not increase security vulnerabilities, that you need to consider.

When you execute the [DeliverPoint Configuration Wizard](#), you provide the name of the SQL Server and the name of the DeliverPoint database. The DeliverPoint configuration wizard then creates the DeliverPoint database. The DeliverPoint database does not need to be created on the same SQL Server instance as the SharePoint databases. Most companies have naming conventions for their databases, and when a company has multiple servers running SQL Server, guidelines as to where databases should be created. Therefore, when you install DeliverPoint in your SharePoint production and integration test environments, you should contact your database administrator (DBA), who will give you the name of the SQL Server and the name for the DeliverPoint database you should use.

You need to provide the [DeliverPoint Configuration Wizard](#) with an Active Directory user id, known as the **DeliverPoint service account**. On the computer where you want to create the DeliverPoint SQL Server database, the *DeliverPoint service account* must be a member of the following [SQL Server roles](#):

- **securityadmin** fixed server role
- **dbcreator** fixed server role

Once the DeliverPoint database is created, these two server roles can be removed from the *DeliverPoint Service Account*. If you want to run Windows PowerShell® cmdlets that affect the database, the account that is used to run the cmdlets must be a member of the **db_owner** fixed database role for the database.

[Go to top of section →](#)

SharePoint server

The [Microsoft® SharePoint® 2013](#) related components of [DeliverPoint 2013](#) are packaged as a SharePoint farm solution, and therefore cannot be installed in [Office 365™](#). DeliverPoint uses [Windows® Installer](#) service to copy the [DeliverPoint binaries](#) to a specified location and creates a shortcut to the [DeliverPoint configuration wizard](#) on the Start Menu. The configuration wizard creates the DeliverPoint database, adds and then deploys the DeliverPoint SharePoint® farm solution. Then the DeliverPoint user interface (UI) feature is activated for each Web Application and five [SharePoint® timer jobs](#) are created:

- Two [interrogator](#) timer jobs,
- [Job Execution](#) timer job.
- [Alerts Processing](#) timer job.
- [Permissions Auditing](#) timer job.

✿ **Note** the two timer jobs [Alerts Processing](#) and [Permissions Auditing](#) were first added when the [Audit Permissions](#) functionality was included in [DeliverPoint version 15.10.5](#). If you are using a [version of DeliverPoint](#) earlier than this version, you will only see three timer jobs.

As DeliverPoint is not implemented as a service application, and DeliverPoint isn't targeting a specific web application, the timer jobs are associated with the Central Administration Web Application.

You only need to run the [DeliverPoint 2013 MSI](#) and the [DeliverPoint Configuration Wizard](#) on one SharePoint server. Lightning Tools recommend these are executed on the server which is hosting the SharePoint 2013 Central Administration web site. All files, such as DeliverPoint _layout pages, are distributed to each SharePoint server via SharePoint's solution deployment mechanism.

To install or upgrade DeliverPoint 2013, you need full access rights to the SharePoint farm configuration database, and therefore you need to use the SharePoint farm administrator account to install DeliverPoint.

✿ **Note** you need to use the same security context to uninstall DeliverPoint that was used to install DeliverPoint. Ensure you record the account used to install DeliverPoint so that if you need to uninstall DeliverPoint, you can use the [DeliverPoint configuration wizard](#) to uninstall DeliverPoint. DeliverPoint can be uninstalled manually using any security context.

Active Directory and SharePoint Interrogation

DeliverPoint interrogates both Active Directory and the SharePoint farm, using two [SharePoint timer jobs](#):

- **Authentication Store Interrogation.** All Active Directory domains and Forests registered with DeliverPoint 2013 will be fully interrogated. The information is extracted in a read-only fashion and the pertinent information, such as is required for *Discover Object Permissions* to show Domain Group membership when an account is added to SharePoint via nested Domain Groups, is stored in the DeliverPoint database. The **DeliverPoint service account** is used to crawl Active Directory. As the *DeliverPoint service account* is an Active Directory user account, and any Active Directory user account has read only access to Active Directory, no special Active Directory configuration is needed for the DeliverPoint Authentication Store timer job to extract the information. However, you should verify that the ports [3268 and 389](#) are open in the firewalls of your SharePoint server(s) and your Active Directory server(s). The load placed on your domain controllers is not substantial.

Additionally, DeliverPoint 2013 also supports Forms Based Authentication (FBA). DeliverPoint 2013 automatically discovers whether Web Applications are configured to use FBA stores, and proceeds to gather all the necessary information for the interrogation, efficiently crawling and obtaining users and roles information from FBA stores.

Note You can use the standalone program, [DPChecker](#), to check your interrogation configuration prior to installing and configuring DeliverPoint.

- **SharePoint Interrogation.** DeliverPoint interrogates all SharePoint content databases in the SharePoint farm using the SharePoint Object Model (OM) and Application Programming Interfaces (API's), and extracts, in a read-only fashion, the pertinent information needed for DeliverPoint to perform functions across an entire farm. The SharePoint content databases are not changed or read directly during the interrogation process. As the interrogation process moves through the farm, the process will interrogate an entire Web Application's contents before moving on to the next Web Application. In other words, the interrogation process performs a deep dive crawl on all the managed paths, site collections, and sites (webs) existing in the Web Application before moving on to the next Web Application. The extracted information is placed into the DeliverPoint database. The account used to run SharePoint timer jobs (SharePoint farm account) is used to interrogate all Web Applications on your SharePoint farm.

The interrogation of both SharePoint and Active Directory is subject to physical network limitations; for example, a domain controller only accessible over a low-speed WAN will take longer to crawl than a single-server setup. Also, the [length of time](#) that it takes for DeliverPoint to interrogate SharePoint is dependent on the number of objects (site collections, webs, lists, etc.) rather than the size of the content databases. A farm with five million objects will take longer to interrogate than a farm with five thousand.

✿ **Note** Domains may be excluded from the Active Directory interrogation to improve interrogation performance.

You cannot use DeliverPoint until a full crawl of both Active Directory and SharePoint is complete. Lightning Tools recommend that you complete this initial full crawl when DeliverPoint interrogation will not have a detrimental affect on other processes which need Active Directory and SharePoint access, such as [user profile synchronization](#) or [full crawls of SharePoint content sources](#). Lightning Tools recommend that you schedule full crawl interrogation to occur at night or another time that suits the SharePoint load, to mitigate any performance concerns you may have if you choose to execute the integration during business hours. Once the initial full crawl of both Active Directory and SharePoint is complete, the SharePoint Interrogation timer job can be configured for incremental crawls.

There are two types of interrogation – incremental and full.

- Full interrogation clears the related tables in the DeliverPoint database and then crawls all objects.
- An incremental interrogation crawls all objects found to have been changed since the last interrogation. For the SharePoint interrogator, the SharePoint Change Log is used to determine whether or not to crawl a given object.

The *Authentication Store Interrogation* timer job is configured by default to run weekly on a Saturday between 2 a.m. and 2:30 a.m., and the *SharePoint Interrogation* timer job is scheduled to run daily, starting every day between 2 a.m. and 4:45 a.m.

✿ The timer job schedules can be modified to meet your needs.

[Go to top of section →](#)

Job Execution timer job


DeliverPoint 2013 submits a job when a user commits an operation using the DeliverPoint 2013 interface. These jobs are then processed by the *Job Execution* timer job, by using information in the DeliverPoint database, and then using the SharePoint APIs to perform the actions against the objects in the SharePoint databases. The *Job Execution* timer job is scheduled to run every 5 minutes.

✿ The Job Execution timer job schedule can be modified to meet your needs.

[Go to top of section →](#)

Alerts Processing timer job


The *Alerts Processing* timer job is configured by default to run every 5 minutes.

 The timer job schedules can be modified to meet your needs.

[Go to top of section →](#)

Permissions Auditing timer job

The *Permissions Auditing* timer job is configured by default to run every 5 minutes.

 The timer job schedules can be modified to meet your needs.

[Go to top of section →](#)

[<< DeliverPoint 2013](#)

[Performance Testing Scenarios >>](#)

[Installation Steps →](#)

Performance Testing Scenarios

Interrogation Performance: The initial interrogation requires a full control permissions of the entire SharePoint® farm. Subsequent interrogations are performed incrementally, resulting in shorter interrogation times and better performance based on changes in SharePoint since the last interrogation.

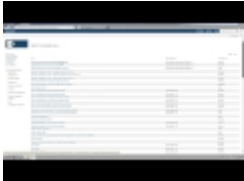
The following interrogation performance information is for an initial interrogation.

The DeliverPoint initial interrogation performance has been tested against a farm with 4 Web Applications, 55 site collections, 39,051 sites, 351, 655 lists, 100 folders, 7,832,692 list items, and 230,000 users (with broken inheritance throughout). In this environment, the DeliverPoint interrogation took a total time of 4h 28m 35s.

[<< Deploying DeliverPoint 2013
Installation Steps >>](#)

Installation Steps

Before installing or upgrading DeliverPoint 2013 you should read the section: [Deploying DeliverPoint 2013](#), then return to this section to install [DeliverPoint 2013](#). You can also view the following video to see how to install DeliverPoint 2013:



The installation of [DeliverPoint](#) is a five step process:

1. [Install DeliverPoint binaries.](#)
2. [Run the DeliverPoint Configuration Wizard.](#)
3. [Configure the DeliverPoint SharePoint® timer jobs to commence a full crawl of Active Directory® and your SharePoint® farm.](#) Once the full crawl is complete, set the [SharePoint interrogator timer jobs for incremental crawls.](#)
4. [Check the DeliverPoint installation.](#)
5. [Activate your DeliverPoint license.](#)

Once you have successfully completed the above steps, if you create a new SharePoint web application, and you want to use DeliverPoint on the new web application, you must complete the following tasks:

1. [Deploy](#) the *lightningtools.deliverpoint.web.ui.wsp* farm solution to the new web application.
2. [Commence a full crawl of your SharePoint® farm](#)
3. [Check that you can use DeliverPoint on the new web application.](#)

[Go to top of section →](#)

[Deploying DeliverPoint 2013 →](#)

[Install the DeliverPoint binaries >>](#)

Install the DeliverPoint binaries

This section documents how to install the DeliverPoint binaries in your organization. You should read the [previous section](#) before completing these steps.

! You must be logged on to a SharePoint Server, preferably the server where the SharePoint 2013 Central Administration web site is hosted, as a SharePoint farm administrator. Also confirm you have local administrator rights on the SharePoint Server to install DeliverPoint.

To install or upgrade/repair [DeliverPoint](#), complete the following steps:

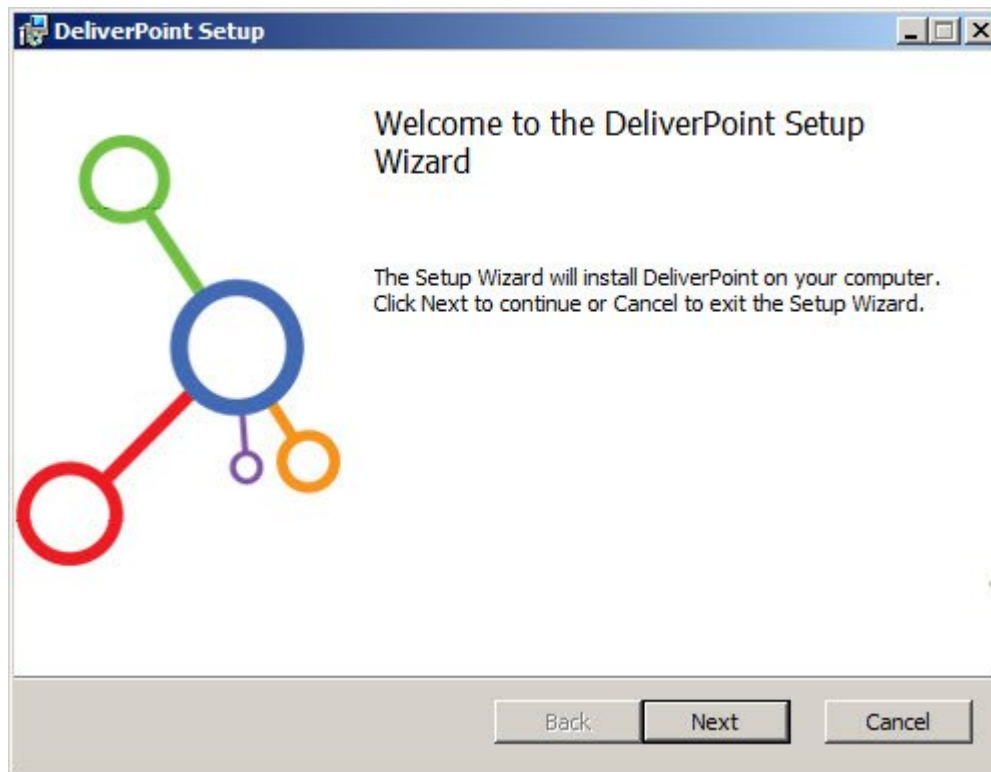
! DO NOT Install or uninstall DeliverPoint during production hours, as both activities initiate an IISRESET.

DO NOT Run the DeliverPoint MSI on every SharePoint Server; the files are distributed to each server via a SharePoint solution deployment.

DO NOT Attempt an install DeliverPoint after an uninstall has failed; see the document Manual Uninstall Steps.

DO NOT Attempt to install DeliverPoint on a server which does not have SharePoint configured.

1. Download the latest version of **DeliverPoint.zip** from your customer portal or the [download section](#) of our web site.
2. Unzip **DeliverPoint.zip** to a suitable location, such as the desktop.
3. Execute **DeliverPoint.msi**, which can be found in the root of the zip file.
The DeliverPoint installation wizard is launched and displays the **Welcome** step.

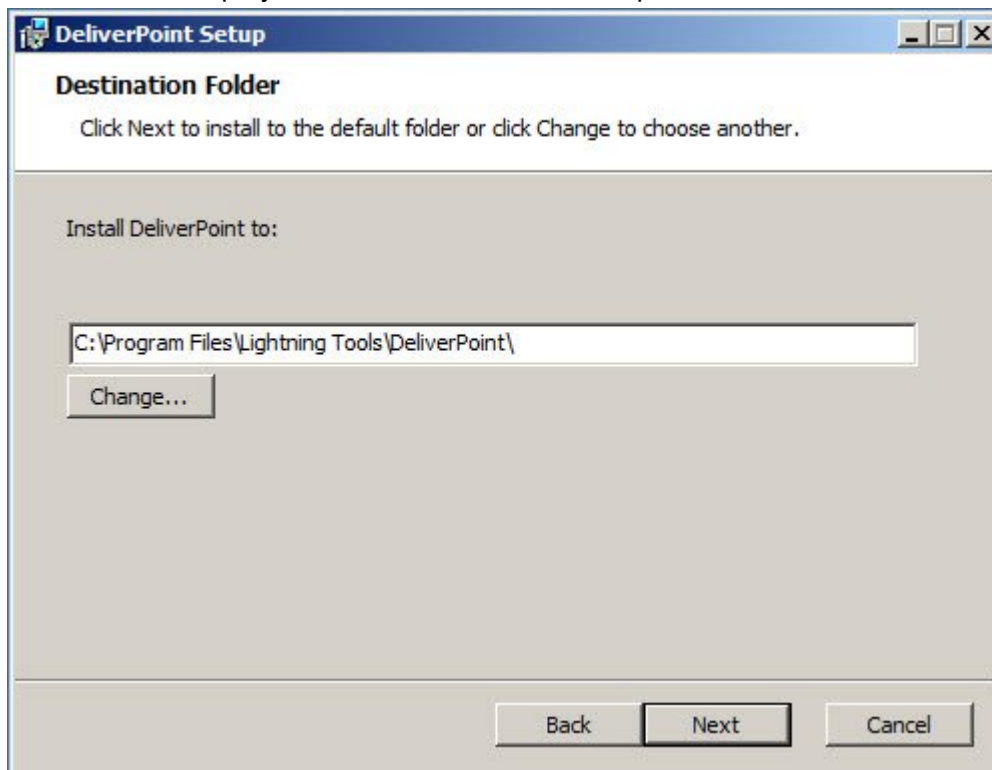


4. Click **Next**.

5. Select the **I accept** check box to agree to the **License Agreement**



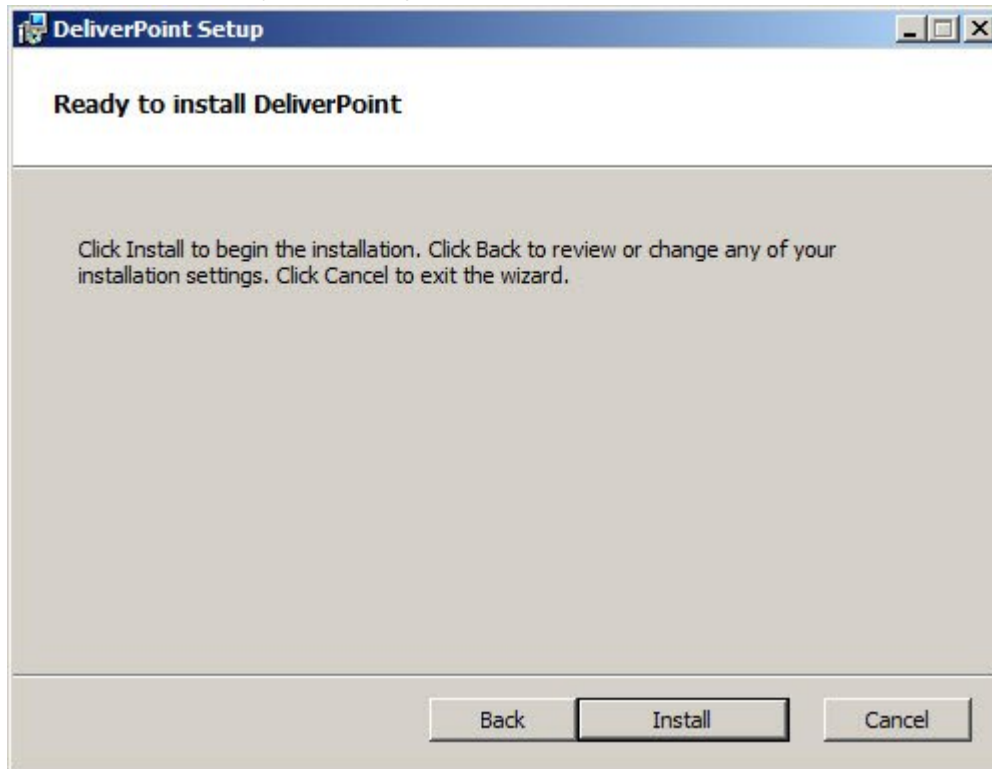
6. Click **Next** to display the **Destination Folder** step.



If you do not want DeliverPoint binaries of DeliverPoint to be deployed in the default location:

c:\Program Files\Lightning Tools\DeliverPoint, click **Change**, select a folder where you want the binaries to be deployed, and then click **OK** to close the **Change destination folder** dialog box.

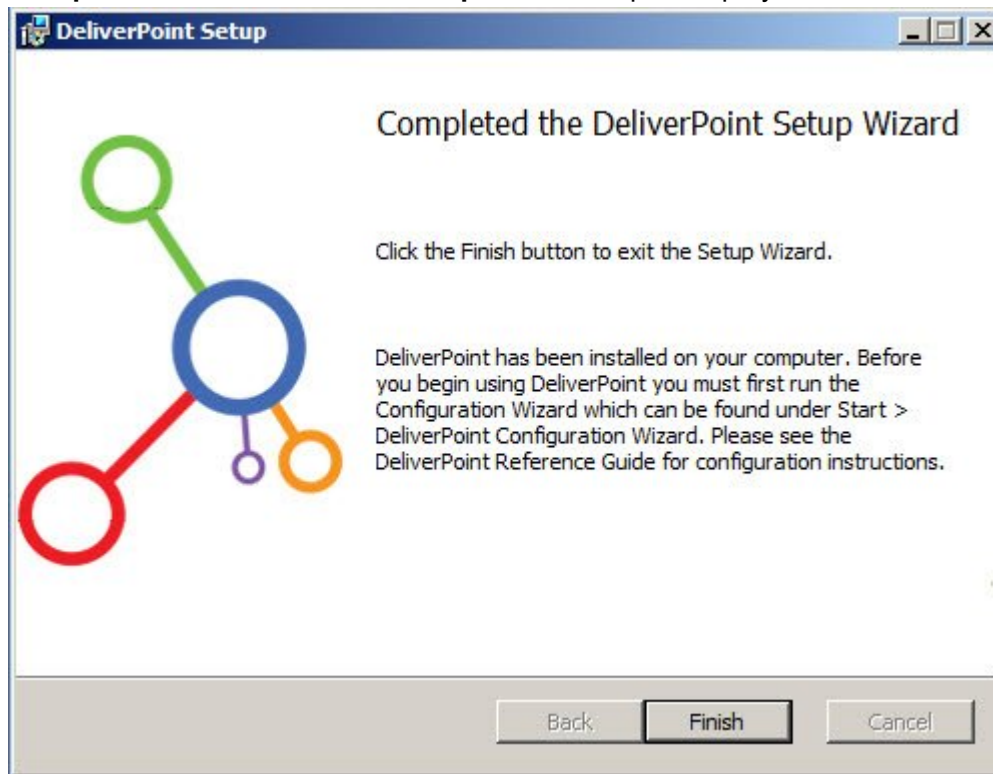
7. Click **Next** to display the **Ready to install DeliverPoint** step.



8. Click **Install**. If the **User Account Control** dialog box is displayed, click **Yes**.

The DeliverPoint 2013 wizard displays the progress of the installation, and when it is finished the

Completed the DeliverPoint Setup Wizard step is displayed.



9. Click **Finish**.

[Go to top of section →](#)

[<< Installation Steps](#)

[DeliverPoint Configuration Wizard >>](#)

[Deploying DeliverPoint →](#)

DeliverPoint Configuration Wizard

The DeliverPoint Configuration Wizard provides a user interface that presents information on how to configure the installation and obtains information from you about the pending installation process. Ensure you read each screen carefully before clicking **Next** to move to the next screen.

! You must be logged on to the SharePoint Server, where you [installed the DeliverPoint binaries](#), as a SharePoint farm administrator.

Before you start the DeliverPoint configuration process, be sure to complete the following:

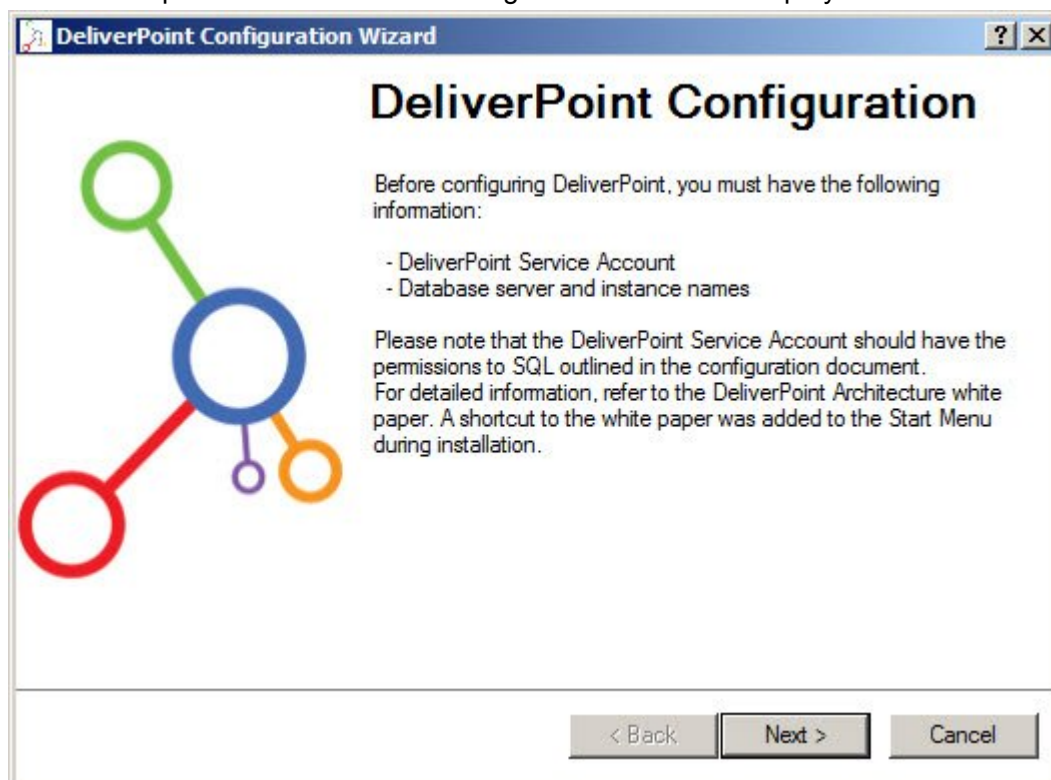
- [Install the DeliverPoint binaries](#).
- Create a Active Directory (AD) username for the DeliverPoint service account, and ensure that it is NOT disabled in AD.
- Inform your database administrator (DBA) that the DeliverPoint configuration wizard will create a new database, and ensure the DeliverPoint service account, you created in the above point, has the [dbcreator and securityadmin server role](#) on the SQL Server where the database is to be created.
- Confirm the [SharePoint Administration](#) (SPAdminV4) service is running successfully on all your Web Front-ends.
- The DeliverPoint service account also requires Read-Write access to the **DeliverPointInstall.log** file, which is created in the *Temp* folder for the userid that you used to install DeliverPoint. The configuration of DeliverPoint will fail if the service account does not have this permission to the *Temp* folder, which is set by an environmental variable that by default is set to *AppData\Local\Temp*. Therefore, navigate to folder set by the TEMP environment variable, such as, C:\Users\<install account>\AppData\Local folder and alter the security properties of the **Temp** folder for the DeliverPoint service account. If there are any errors during the configuration of DeliverPoint you will see them in the *DeliverPointInstall.log* file, for example, if you have not provided the DeliverPoint read-write access to the *Temp* folder, the error message in the *DeliverPointInstall.log* file, will be similar to:

```
Running database setup
SERVER: sql1.trainsbydave.com; DATABASE DP2013; User: trainsbydave\
dpSERVICE
Impersonating user
System.UnauthorizedAccessException: Access to the path 'C:\Users\brett.DP\
AppData\Local\TempDeliverPointInstall.log' is denied.
```

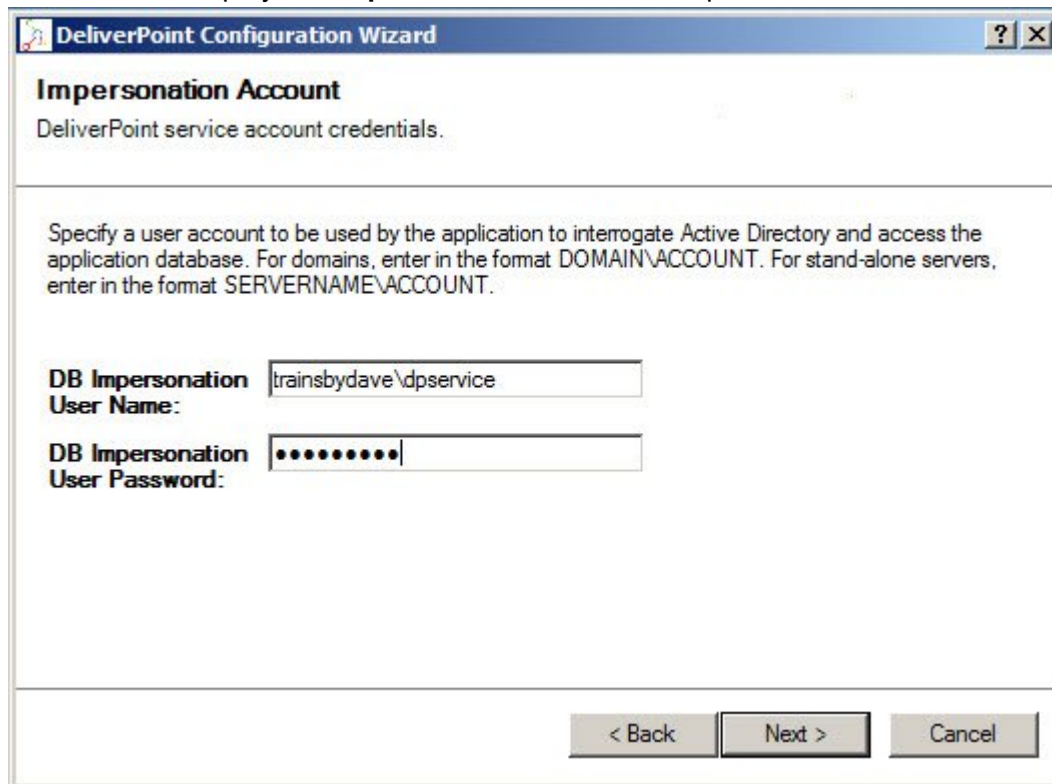
To configure DeliverPoint use the following steps:

1. Once you have installed the DeliverPoint binaries, start the DeliverPoint Configuration Wizard, which you can find on:
 - Windows Server® 2008 by clicking **Start, All Programs, DeliverPoint Configuration Wizard** and there should be a shortcut to the configuration wizard on your desktop.
 - Windows Server® 2012, you can find the **DeliverPoint Configuration Wizard** on the **Start** screen.
3. If the **User Account Control** dialog box is displayed, click **Yes**.

The first step of the DeliverPoint Configuration Wizard is displayed.



- Click **Next** to display the **Impersonation Account** step.




The screenshot shows a Windows-style dialog box titled "DeliverPoint Configuration Wizard". The main heading is "Impersonation Account" with the subtitle "DeliverPoint service account credentials." Below this, a text block instructs the user: "Specify a user account to be used by the application to interrogate Active Directory and access the application database. For domains, enter in the format DOMAIN\ACCOUNT. For stand-alone servers, enter in the format SERVERNAME\ACCOUNT." There are two input fields: "DB Impersonation User Name:" containing the text "trainsbydave\dpSERVICE" and "DB Impersonation User Password:" containing a series of dots. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

- In the **DB Impersonation User Name** text box, type the DeliverPoint service account credentials. Use the *DOMAIN\username* format to enter the AD account.
- In the **DB Impersonation User Password** text box, type the password of the service account.
- If you have previously installed DeliverPoint then a checkbox is displayed which when selected allows you to save the previous installation settings.
- Click **Next**.

The configuration wizard checks that the you have entered a valid AD account and that you have not previously installed DeliverPoint. If the credentials are not valid, then a **Invalid Credentials** dialog box is displayed, click **OK** and then enter valid AD credentials and then click **Next**.

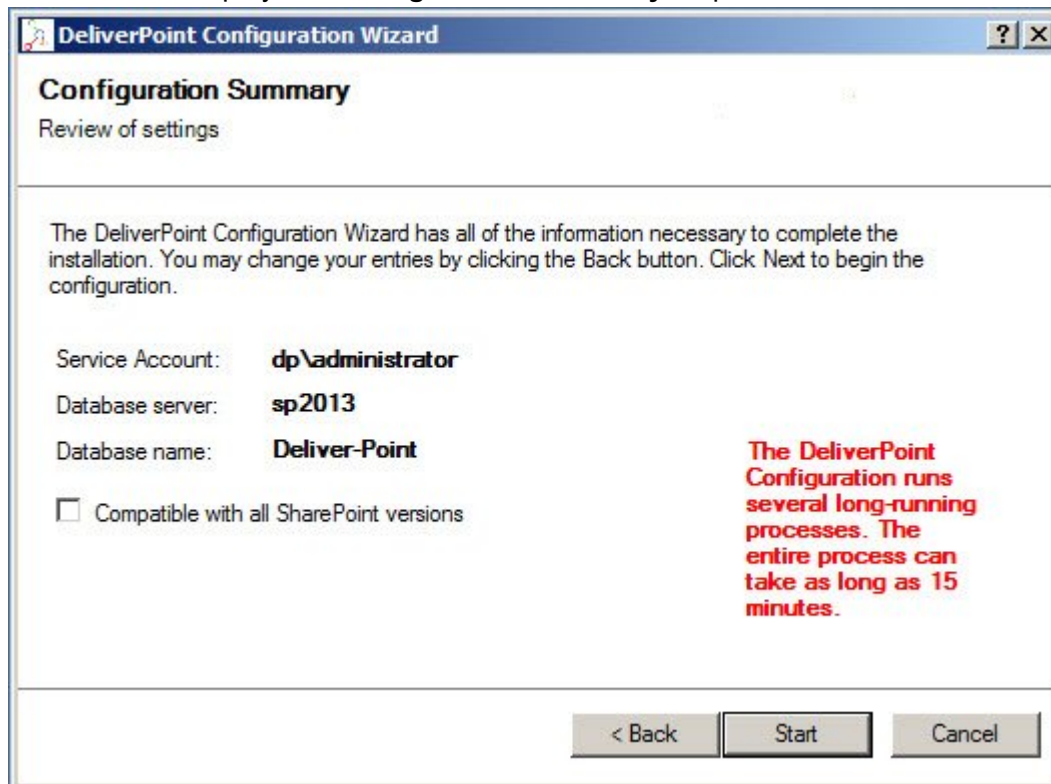
The **Database Configuration** step. is displayed.



The screenshot shows a Windows-style dialog box titled "DeliverPoint Configuration Wizard". The main heading is "Database Configuration", and the subtitle is "Server Name and Database Name". The text inside the dialog states: "DeliverPoint requires a Microsoft SQL Server database to store information about your farm, scheduled jobs and application information. Please enter the name of the server and database." There are two text input fields: "Server Name:" with the value "sql1.trainsbydave.com" and "Database Name:" with the value "DeliverPoint". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

- In the **Server Name** text box, type the name of the server running SQL Server where the DeliverPoint database should be created.
- In the **Database Name** text box, type the name of the DeliverPoint database.

9. Click **Next** to display the **Configuration Summary** step.



10. Optionally choose "Compatible With All SharePoint Versions". If you have performed an upgrade from SharePoint 2010 to 2013 for example and still have some team sites or pages using the SharePoint 2010 look and feel. DeliverPoint will adhere to both master pages if this option is selected.
11. Check that the details are correct, and then click **Next** to complete the installation, that is:
- The DeliverPoint database is created.
 - The DeliverPoint SharePoint® farm solution is added and deployed.
 - The DeliverPoint user interface (UI) is activated for each Web Application.
 - The three SharePoint® timer jobs are installed.
- This process could take between 5-15 minutes to complete. When complete the **Configuration Complete** message is displayed.

1. Click **Next** to display the **Success** step, and then click **Finish**.



[<< Install the DeliverPoint binaries](#)

[Commence Full crawl of Active Directory and SharePoint >>](#)

[Deploying DeliverPoint →](#)

[Installation Steps →](#)


Commence Full crawl of Active Directory and SharePoint

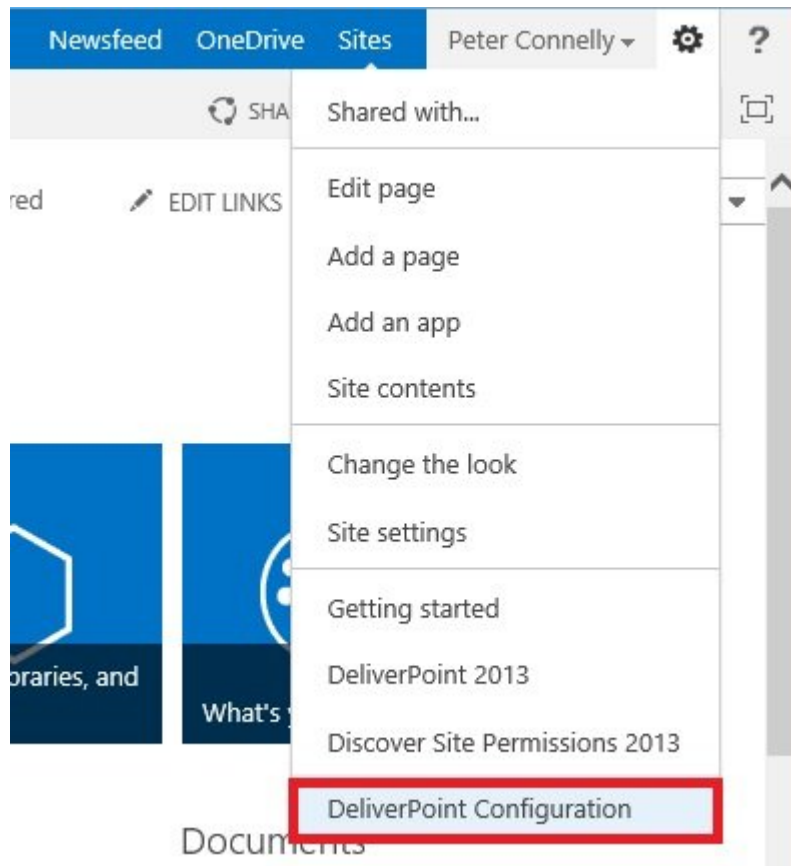
DeliverPoint interrogates both Active Directory and the SharePoint farm, using two SharePoint timer jobs. You must ensure that the DeliverPoint Service Account that you entered in the [DeliverPoint Configuration Wizard](#) was granted [Full Control permissions on all Web Applications](#) you wish to crawl, and verify the ports [3268 and 389](#) are open between your SharePoint server(s) and your Active Directory server(s).



If you wish to check the Active Directory authentication interrogation prior to initiating a full crawl of Active Directory, then use the [DeliverPoint Checker](#) standalone program.

Use the following steps to configure DeliverPoint timer jobs to start a full crawl of your Active Directory and SharePoint farm.

1. In the browser, open Microsoft SharePoint 2013/2016 Central Administration web site.
2. Click **Settings**  , and then click **DeliverPoint Configuration** to display the **DeliverPoint Configuration** page



If you do not see the three new DeliverPoint options on the *Settings* menu, refresh the browser. The [DeliverPoint Configuration](#) page is displayed.

3. Click **TimerJob Settings**.

[Lightning Tools](#) > DeliverPoint 2013 Configuration

DeliverPoint Configuration ⓘ

Forest Settings

Manage forests and domains registered for crawl. Add/delete new forests and domain registrations, change access credentials.



Treeview Settings

Update the settings for the DeliverPoint Treeview.



Threshold Settings

Update the DeliverPoint threshold settings - update thresholds for the size and age of web applications, wait interval after each interrogation and other settings.



Permission

Update the settings for the Permissions module. Specify the site collection administrator replacement and specify DeliverPoint operators.



TimerJob Settings

Update the settings for the DeliverPoint timer jobs. Specify the interrogations logging level, SharePoint interrogation type.



4. On the **DeliverPoint timer job settings** page, in the **SharePoint crawl method** section, select **Full**.

[Lightning Tools](#) > [DeliverPoint 2013 Configuration](#) > [Timer Jobs](#)

DeliverPoint timer job settings ⓘ

SharePoint crawl method

Specify SharePoint crawler method - full or incremental. Incremental crawl is recommended, if SharePoint Farm is big.

☒ Full: Deletes old crawled data and performs new full SharePoint crawl

☐ Incremental: Performs partial crawl over the changed content only

Logging level

Control logging level for all timer jobs.

Logging Level:

☐ Deep: log info, warning and error messages

☒ Errors: log only error messages

Exclusions List/Library Types

Mark list types to be excluded from permission scans

Exclude List Types:

- ☐ NoListTemplate
- ☐ GenericList
- ☐ DocumentLibrary
- ☐ Survey
- ☐ Links
- ☐ Announcements
- ☐ Contacts

5. Scroll to the bottom of the page, and click **OK** to redisplay the **DeliverPoint Configuration** page.
6. In the breadcrumb, click **Central Administration**. On the Quick Launch click **Monitoring**, and then under **Timer Jobs**, click **Review job definitions**.



Monitoring

Central Administration

Application
Management

System Settings

Monitoring

Backup and Restore

Security

Upgrade and Migration



Health Analyzer

[Review problems and solutions](#) | [Review rule definitions](#)



Timer Jobs

[Review job definitions](#) [Check job status](#)



Reporting

[View administrative reports](#) | [Configure diagnostic logging](#) |
[Configure usage and health data collection](#) | [View health reports](#)

7. On the **Job Definitions** page, check that the five LightningTools DeliverPoint timer jobs were deployed on the SharePoint Central Administration Web Application:

- DeliverPoint Alerts Processing.
- DeliverPoint Authentication Store Interrogation.
- DeliverPoint Job Execution.
- DeliverPoint Permissions Auditing.
- DeliverPoint SharePoint Interrogation.

Tip: Use the **View** and **Web Application** filters to display only timer jobs associated with the SharePoint Central Administration web application, to quickly find these five timer jobs.



Job Definitions

Timer Links

Timer Job Status

[Scheduled Jobs](#)

[Running Jobs](#)

[Job History](#)

[Job Definitions](#)

Central Administration

Web Application: <http://sp2013:20103/> | View: [Web Application](#)

Title	Web Application	Schedule Type
DeliverPoint Authentication Store Interrogation	SharePoint Central Administration v4	Weekly
DeliverPoint Job Execution	SharePoint Central Administration v4	Minutes
DeliverPoint SharePoint Interrogation	SharePoint Central Administration v4	Daily

6. Click **DeliverPoint Authentication Store Interrogation** to display the **Edit Timer Job** page.

Edit Timer Job

Job Title
DeliverPoint Authentication Store Interrogation

Job Description

Job Properties
This section lists the properties for this job.




Web application:

Last run time: N/A




Recurring Schedule
Use this section to modify the schedule specifying when the timer job will run. Daily, weekly, and monthly schedules also include a window of execution. The timer service will pick a random time within this interval to begin executing the job on each applicable server. This feature is appropriate for high-load jobs which run on multiple servers on the farm. Running this type of job on all the servers simultaneously might place an unreasonable load on the farm. To specify an exact starting time, set the beginning and ending times of the interval to the same value.

This timer job is scheduled to run:

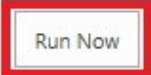


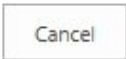
☐ Minutes Starting every week between

☐ Hourly Saturday  at 2 AM  00 

☐ Daily and no later than

☒ Weekly Saturday  at 2 AM  30 

☐ Monthly

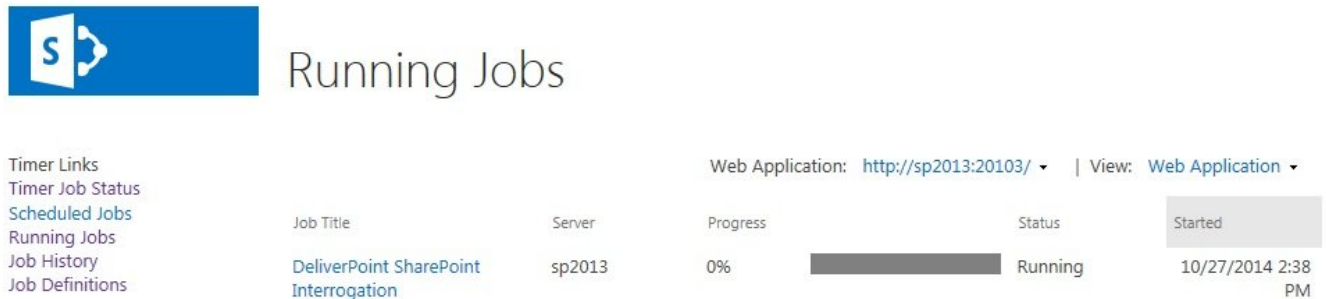
7. At the bottom of the page, click **Run Now**.
8. The interrogation of your Activate Directory may take some time. To check when the authentication crawl is complete, on the Quick Launch, click **Running Jobs** under **Timer Links**. When the **Authentication Store Interrogation** timer job is no longer displayed on the page, continue with the next steps.

Tip: If you are unsure whether the job ran, on the Quick Launch, click **Job History** under **Timer**

Links, and check that the **Authentication Store Interrogation** timer job run and has a *Status* of **Succeeded**.

9. On the Quick Launch, click **Job Definitions** and then click **DeliverPoint SharePoint Interrogation**.
10. At the bottom of the **Edit Timer Job** page, click **Run Now**.


The interrogation of your SharePoint Web Applications may take [some time](#). To check when the SharePoint crawl is complete, on the Quick Launch, click **Running Jobs** under **Timer Links**.



The screenshot shows the 'Running Jobs' page. On the left is a sidebar with 'Timer Links' and a list of links: 'Timer Job Status', 'Scheduled Jobs', 'Running Jobs' (highlighted), 'Job History', and 'Job Definitions'. The main area has a header with 'Web Application: http://sp2013:20103/' and 'View: Web Application'. Below this is a table with columns: 'Job Title', 'Server', 'Progress', 'Status', and 'Started'. One job is listed: 'DeliverPoint SharePoint Interrogation' on server 'sp2013', with '0%' progress, 'Running' status, and 'Started' on '10/27/2014 2:38 PM'.

Job Title	Server	Progress	Status	Started
DeliverPoint SharePoint Interrogation	sp2013	0%	Running	10/27/2014 2:38 PM

When the **SharePoint Interrogation** timer job is no longer displayed on the page, continue with the next steps.

11. Click **Settings** , and then click **DeliverPoint Configuration** to display the **DeliverPoint Configuration** page.
12. Click **TimerJob Settings**.
13. In the **SharePoint crawl method** section, select **Incremental** and then at the bottom of the page, click **OK** to redisplay the **DeliverPoint Configuration** page.
14. If the default schedules for the five DeliverPoint timer jobs do not suit your organization, go to the **Job Definition** page, and modify them.

[Go to top →](#)

[<< DeliverPoint Configuration Wizard](#)


[Check the DeliverPoint installation >>](#)

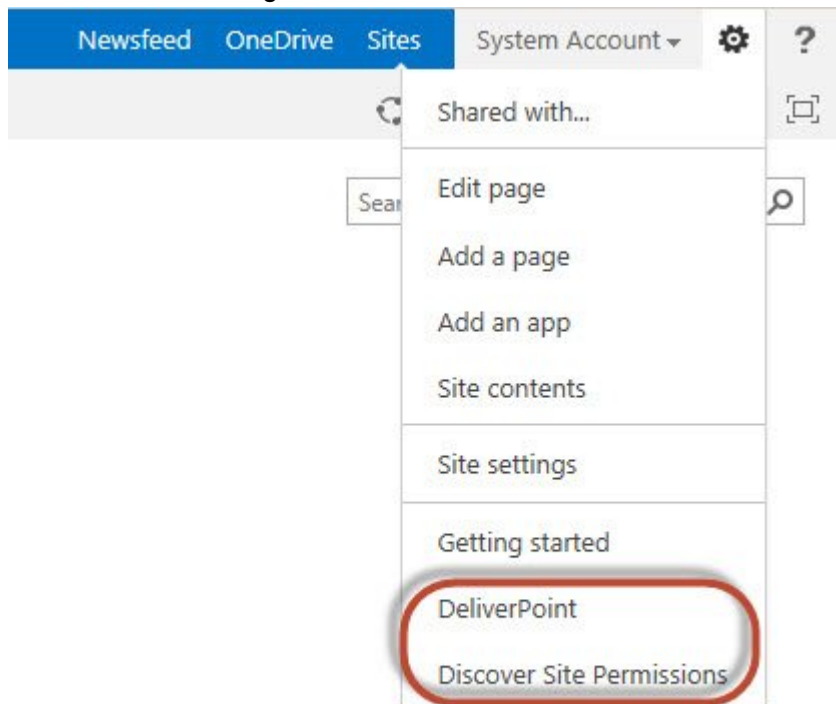
[Deploying DeliverPoint →](#)

[Installation Steps →](#)

Check the DeliverPoint installation

Use the following steps to check that [DeliverPoint is correctly installed](#) and that the [two interrogation timer jobs](#) ran successfully.


1. In the browser, navigate to a SharePoint site, click **Settings** . You should see two links at the bottom of the Settings menu: **DeliverPoint 2013** and **Discover Site Permissions 2013**.



Note: If you are using the SharePoint 2013 Central Administration web site and you are a SharePoint farm administrator you will see a third DeliverPoint link: *DeliverPoint Configuration*.

2. Click **Discover Site Permissions 2013** to to open a new browser window displaying the [Discover Permissions](#) page.

Home	Site	User Name	Permissions	Permissioned Via...
Lists	<input type="checkbox"/> Demos	administrator	Full Control (Implicit)	Site Collection Administrators
Documents	<input type="checkbox"/> Demos	Brett	Full Control (Implicit)	Site Collection Administrators
Access Apps	<input type="checkbox"/> Demos	Brett	Full Control (Implicit)	Site Collection Administrators
Asset Tracking	<input type="checkbox"/> Demos	Sara	Full Control (Implicit)	Site Collection Administrators
Issue Tracking	<input type="checkbox"/> Demos	SP Admin	Full Control (Implicit)	Site Collection Administrators
Orders and Products	<input type="checkbox"/> Demos	administrator	Full Control	Teams Owners
Subsites	<input type="checkbox"/> Demos	Brett	Full Control	Teams Owners

3. Click **Settings**  and then click **DeliverPoint 2013**

The main [DeliverPoint dashboard](#) is displayed, where you should see in the tree view each Web Application in your SharePoint farm.

Tree view Results pane

SharePoint Newsfeed OneDrive Sites Brett ?

BROWSE VIEW COMMANDS REPORT

Discover Permissions Permission Inheritance Properties Open Copy Permissions Grant Permissions Transfer Permissions Delete Permissions Dead Accounts Compare Permissions Copy Site Permissions Unique Lists Copy List Permissions View Folders

Comm Account Management Site Management List Management

Demos Web Properties

Aggregate Data

	New	Aging	Old	Empty	Small	Medium	Large
Sites (1)	0	0	1	0	0	0	1
Subsites (27)	0	1	26	0	24	1	2
Lists (243)	0	17	226	6	230	5	2



Last Interrogation: 27 OCT at 02:41PM



Demos Site

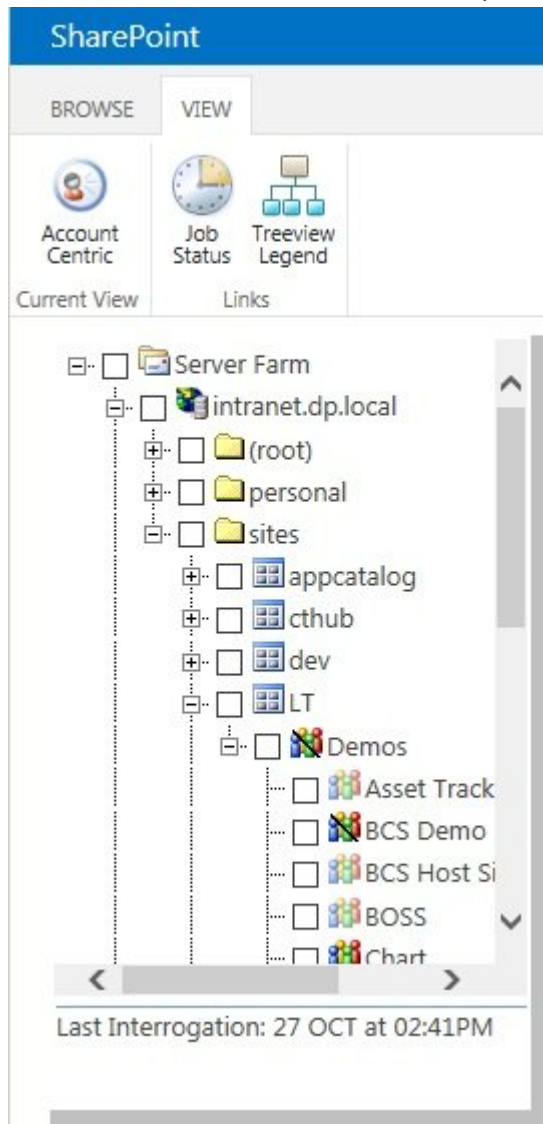
Sites and Workspaces:16
Recycle Bin:2

Permission Inheritance:Unique
Permissions Managed By:Demos
Last Modified:undefined

Interrogation status area Properties pane

4. Click the plus sign (+) to the left of a Web Application  , and continue to click the plus signs to expand the objects under the Web Application. Check that you can see managed paths  , site

collections  , and sites  . This proves that the SharePointIntegration crawl was successful.



[Goto top →](#)

References

[<< Commence Full crawl of Active Directory and SharePoint](#)

[Activating your DeliverPoint License >>](#)

[Deploying DeliverPoint →](#)

[Installation Steps →](#)

[Permission Management →](#)

Activating your DeliverPoint License

The [DeliverPoint 2013](#) is available as a 14 day trial. You can use the full functionality of the DeliverPoint for 14 days, after which the product will need to be licensed. The number of days remaining in your trial will be shown on the [DeliverPoint Configuration Settings](#) page. After the 14 day period has expired, users will not be able to use DeliverPoint until DeliverPoint is licensed.

You can check the license information on the [DeliverPoint Configuration Settings](#).

* If you have purchased a license of the product already and believe that the information in the [DeliverPoint Configuration Settings](#) is incorrect, please contact Lightning Tools by clicking [Submit Support Ticket](#) on [Lightning Tools](#) web site. We will then gladly provide you with a license key.

When you purchase the DeliverPoint 2013, you will need to inform [Lightning Tools](#) of the number of Web Front-ends and the number of SharePoint farms you wish to purchase a license, including production and non-production Microsoft® SharePoint® environments. We will then provide you with a valid license key for each SharePoint farm where you want to use DeliverPoint.

* For licensing purposes, a SharePoint Web Front-end (WFE) is a server that has the [Microsoft SharePoint Foundation Web Application](#) service started.

Once you have purchased DeliverPoint and have received the license key, you need to enter the key and activate the product via the Lightning Tools license manager which can be found on the **System Settings** page on the SharePoint 2013 Central Administration web site.

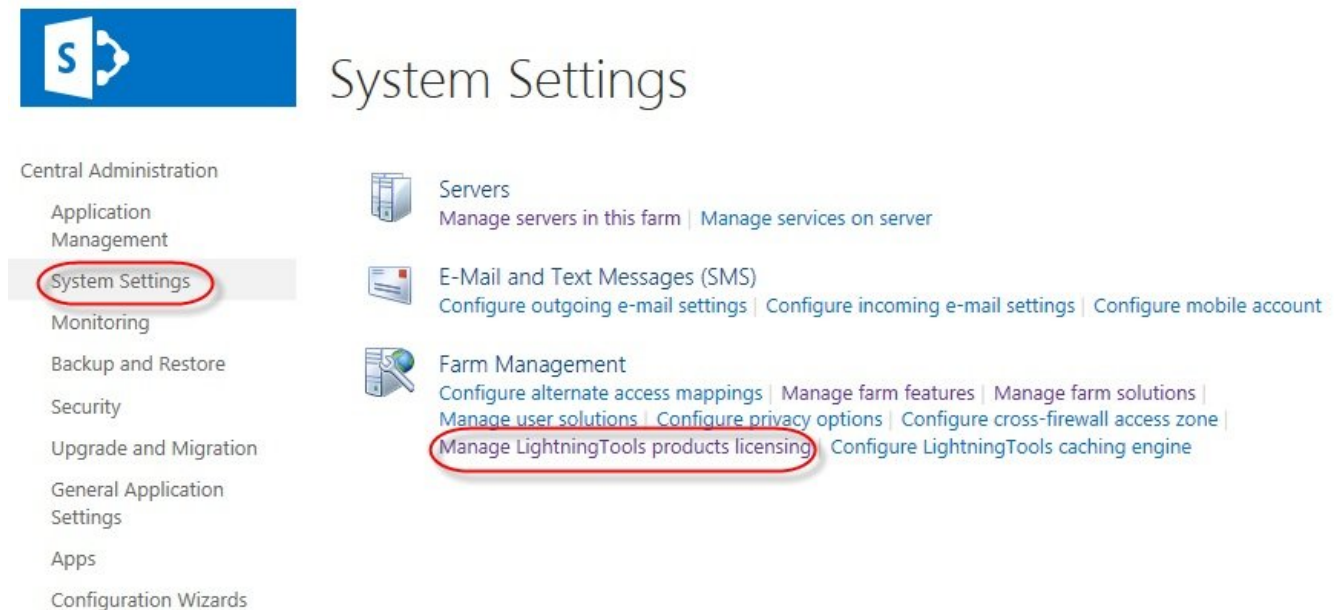
Tip: If the **Manage LightningTools products licensing** link is missing on the **System Settings** page, complete steps similar to those on documented the [Troubleshooting](#) page.

You can activate DeliverPoint over the [Internet](#) or [manually](#). Once a license key is activated, it will be associated with a specific SharePoint farm, and can not be activated on a different SharePoint farm. License keys are also specific to a [Lightning Tools](#) product, therefore you need a license key for each [Lightning Tools](#) product that you install on your SharePoint farm.

Activate with Internet Access

To activate DeliverPoint, automatically when your machine has access to the internet:

1. In the browser, open **SharePoint 2013 Central Administration** web site.
2. On the Quick Launch, click **System Settings**, and then under **Farm Management** click **Manage LightningTools products licensing**.



Tip: If the **Manage LightningTools products licensing** link is missing on the **System Settings** page, complete steps similar to those documented on the [Troubleshooting](#) page.

3. Select the **DeliverPoint 2013** product from the **Choose Product** drop down list.
4. In the **License Key** text box, type the license key sent to you when you [completed your purchase](#) of DeliverPoint.
5. In the **User Email** text box, type your email address.
6. In the **Organization** text box, type your organization or company name.
7. In the **User Name** text box, type your first name and last name.
8. Click **Activate**

The page is redisplayed with a **License Status: The Product is properly licensed**.

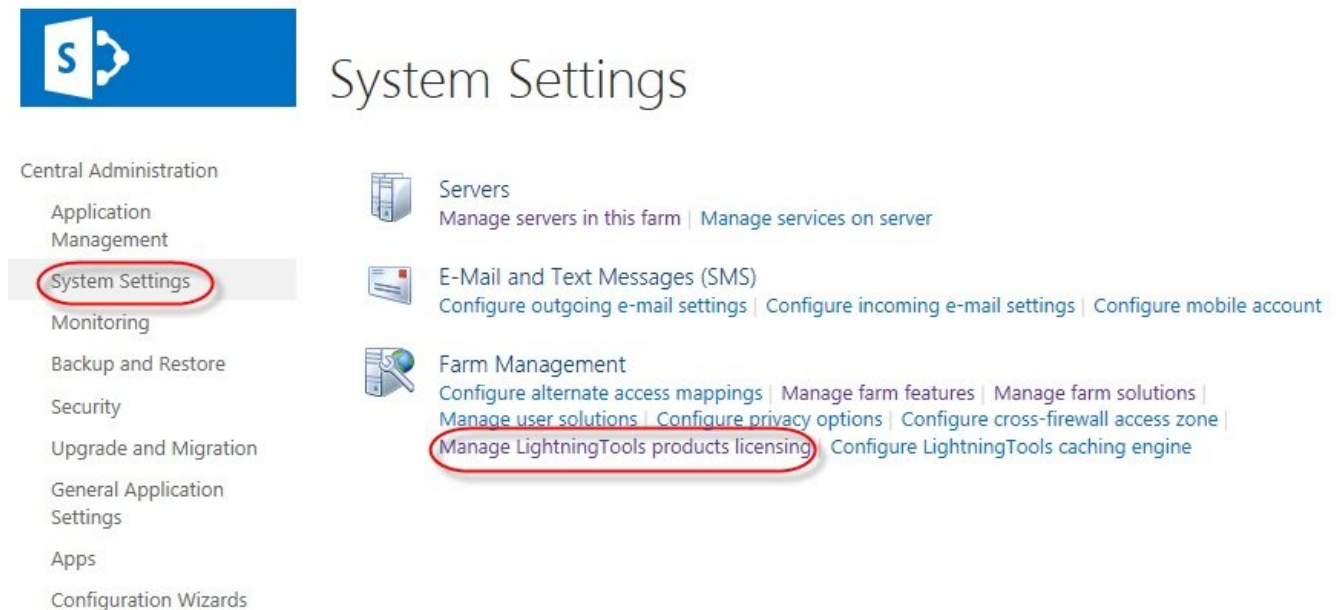
The [DeliverPoint](#) license is now activated and registered with [Lightning Tools](#).

[Go to top →](#)

Activate without Internet Access

To activate DeliverPoint manually when your machine does not have access to the internet:

1. In the browser, open **SharePoint 2013 Central Administration** web site.
2. On the Quick Launch, click **System Settings**, and then under **Farm Management** click **Manage LightningTools products licensing**.



Tip: If the **Manage LightningTools products licensing** link is missing on the **System Settings** page, complete steps similar to those documented on the [Troubleshooting](#) page.

3. Select the **DeliverPoint 2013** product from the **Choose Product** drop down list.
4. In the **License Key** text box, type the license key sent to you when you [completed your purchase](#) of Social Squared.
5. In the **User Email** text box, type your email address.
6. In the **Organization** text box, type your organization or company name.
7. In the **User Name** text box, type your first name and last name.
8. Now complete one of the following steps.
 - If the server that you are using has mail access, click **Send Activation Email** to send an email to Lightning Tools with your identity key and license key, which is used to generate the license.

Or

- Copy the contents from **License Information** text box, and save it in a manner so you have access to that information from another computer.
- On a computer where you can send emails, paste the *License Information* into the body of the email, and send to support@lightningtools.com with a **Subject** line of: **DeliverPoint 2013 activation request**.

Lightning Conductor 2013 activation request

FILE MESSAGE INSERT OPTIONS FORMAT TEXT REVIEW

Clipboard Basic Text

To: support@lightningtools.com

Cc:

Subject: Lightning Conductor 2013 activation for Brett Lonsdale

Key: 0a8bb385-9baf-448d-969e-c4e501c4d9c4-03
 Identity: 9257a238-3090-490b-8e5f-1c22f3a78340
 Product name: Lightning Conductor 2013
 Organization: Lightning Tools
 User name: Brett Lonsdale
 User email: brett@lightningtools.com

Newsfeed SkyDrive Sites System Account

Your trial is valid. 14 days left.

License Key*
 0a8bb385-9baf-448d-969e-c4e501c4d9c4-03

User Email*
 brett@lightningtools.com

Organization
 Lightning Tools

User Name
 Brett Lonsdale

License Information

```
<?xml version="1.0" encoding="utf-16"?>
<License>
  <Id>c69a405b-9474-4788-983a-ea31ee12f4d9</Id>
  <Type>Trial</Type>
  <Expiration>Wed, 14 Aug 2013 13:56:03 GMT</Expiration>
  <ProductFeatures>
    <Feature name="User Identity">9257a238-3090-490b-8e5f-1c22f3a78340</Feature>
    <Feature name="Product">Lightning Conductor 2013</Feature>
  </ProductFeatures>
  <Customer>
```

Send Activation Email Save License Register Online Cancel

4. Activation information will be sent in an email to the email address you provided in step 6. The email contains an XML license which can be pasted in the **License Information** text box replacing the existing contents.
5. Click **Save License**.

The [DeliverPoint](#) license is now activated and registered with [Lightning Tools](#).

[Go to top →](#)

[<< Check the DeliverPoint installation](#)


[How to find the DeliverPoint version >>](#)

[Deploying DeliverPoint →](#)

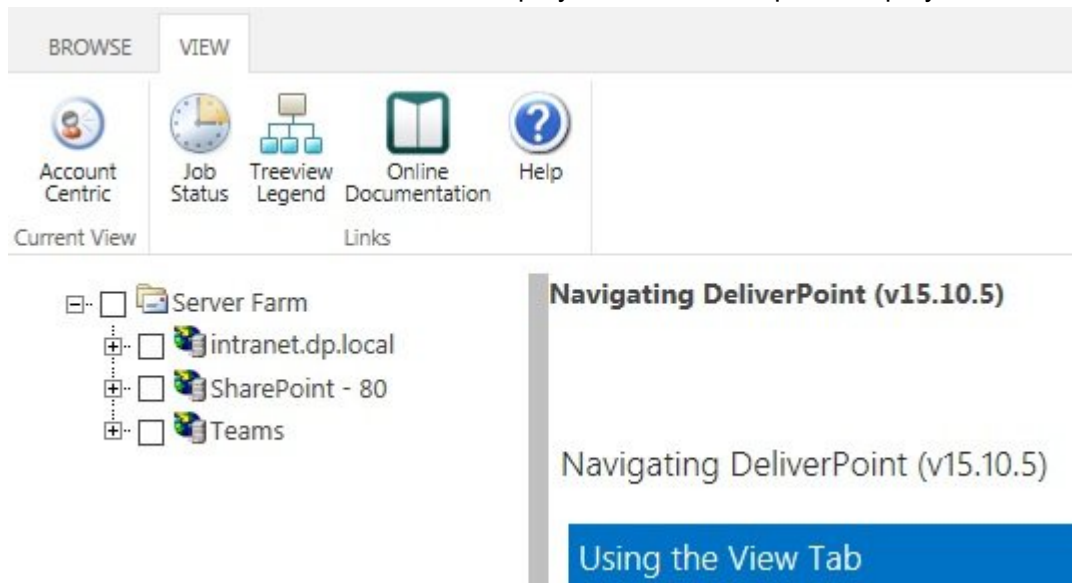
[Installation Steps →](#)

How to find the DeliverPoint version

To find the version of DeliverPoint installed on your SharePoint farm, complete the following steps:

1. In the browser, navigate to a SharePoint site.
2. Click **Settings**  and then click **DeliverPoint 2013**.

The main [DeliverPoint dashboard](#) is displayed. The results pane displays the DeliverPoint version.



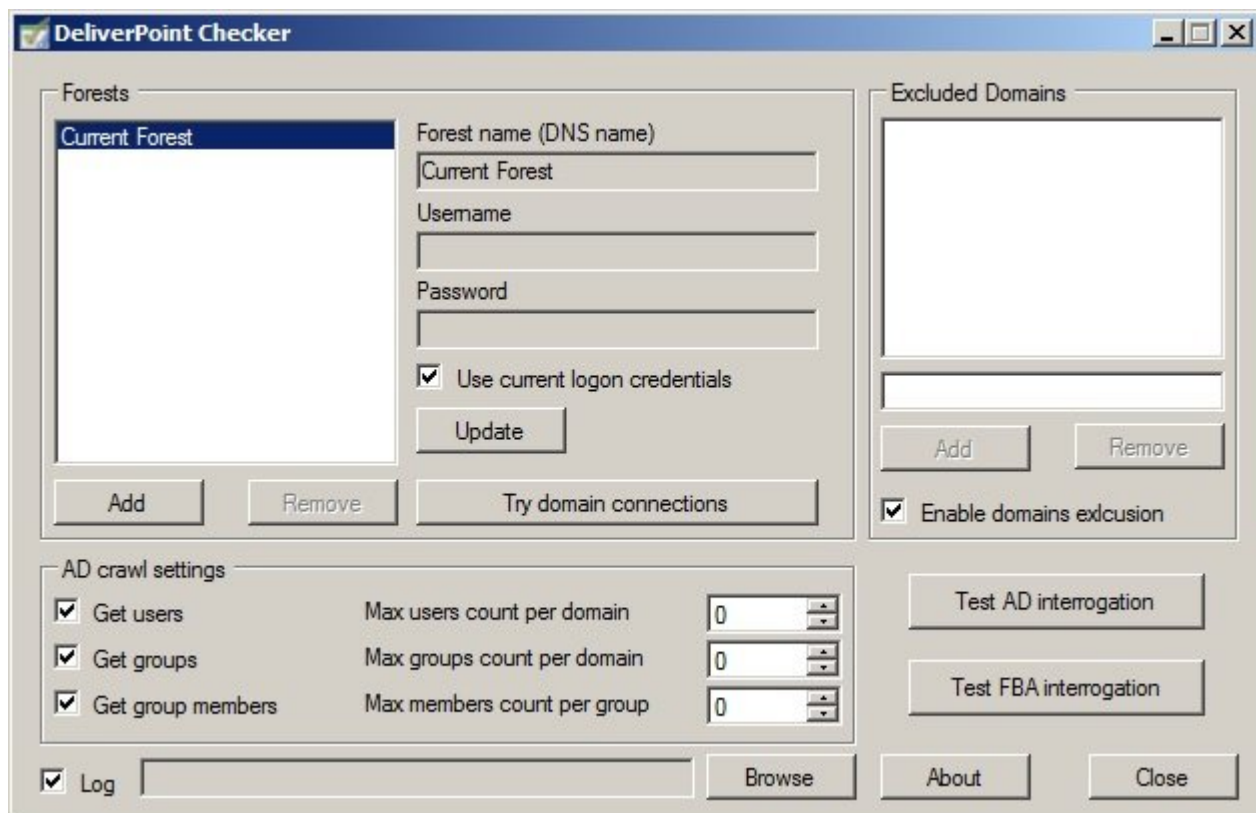
[<< Activating your DeliverPoint License](#)
[DeliverPoint Checker >>](#)

DeliverPoint Checker

DPChecker is a stand-alone desktop application tool which you can use prior to installing DeliverPoint. It helps check an authentication store crawl before configuring the [DeliverPoint Authentication Store Interrogation](#) SharePoint timer job. DPChecker requires the Microsoft .NET Framework 3.5 and SharePoint installed in the same machine.

Use the following steps to use DPChecker:

1. Download the **DeliverPoint zip** file from <http://lightningtools.com/trial-download..>
2. Unzip **DeliverPoint zip** file to a suitable location, such as the desktop.
3. Double click **DPChecker 1.5.exe**.



DPChecker version 1.5 supports three main features:

1. [Test Active Directory Interrogation](#).
2. [Test Forms Based Authentication Stores Interrogation](#).
3. [Try Domain Connections](#).



Without SharePoint installation it will be not possible to use **Test FBA Interrogation** feature.

Test Active Directory Interrogation

The Active Directory Interrogation feature allows you to test an Active Directory (AD) users/groups crawl using a specified configuration. Use the following steps to configure and test AD interrogation:

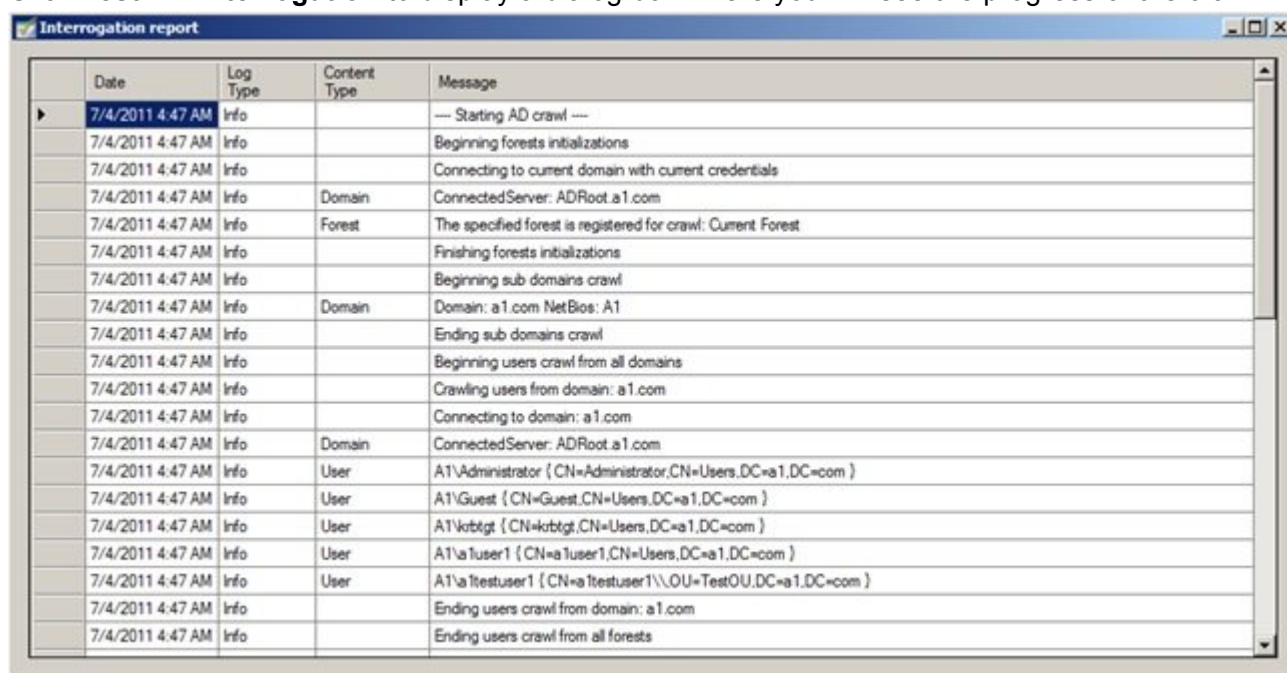
1. In the **Forests** section, if you do not want to use **Current Forest**, complete the following:
 - Click **Add** to create a new entry with an empty configuration.
 - In the **Forest name (DNS name)** text box, type the forest name – you must enter a DNS name.
 - In the **Username** text box, type the AD username, which should be used to perform the specified forest (all its subdomains) users/groups enumeration.
 - In the **Password** text box, type the password.
 - Alternatively you can select **Use current logon credentials** to use current logged in user for the specified forest crawl.
 - Click “Update” to apply new configuration.

If you need to remove a AD forest you previously registered, click **Remove**. You cannot delete the **Current Forest**.

Note: Any time you need to change existing forests registration settings, you must select the forest name from the list, edit the credentials and password, and then click **Update**.

7. If you need to exclude some domains from interrogation, use the **Excluded Domains** section.
 - Add DNS or NetBIOS names of domains you want to exclude.
 - Ensure that “Enable domains exclusion” check box is selected.
8. Use **AD Crawl Settings** section to limit the crawl. Interrogation will stop after reaching the specified count for each operation (0 indicates to no limit).
9. If you want the results of the crawl saved in a log file, select **Log** and then click **Browse** to specify the name and location of the log file.

10. Click **Test AD interrogation** to display a dialog box where you will see the progress of the crawl.



Date	Log Type	Content Type	Message
7/4/2011 4:47 AM	Info		--- Starting AD crawl ---
7/4/2011 4:47 AM	Info		Beginning forests initializations
7/4/2011 4:47 AM	Info		Connecting to current domain with current credentials
7/4/2011 4:47 AM	Info	Domain	ConnectedServer: ADRoot.a1.com
7/4/2011 4:47 AM	Info	Forest	The specified forest is registered for crawl: Current Forest
7/4/2011 4:47 AM	Info		Finishing forests initializations
7/4/2011 4:47 AM	Info		Beginning sub domains crawl
7/4/2011 4:47 AM	Info	Domain	Domain: a1.com NetBios: A1
7/4/2011 4:47 AM	Info		Ending sub domains crawl
7/4/2011 4:47 AM	Info		Beginning users crawl from all domains
7/4/2011 4:47 AM	Info		Crawling users from domain: a1.com
7/4/2011 4:47 AM	Info		Connecting to domain: a1.com
7/4/2011 4:47 AM	Info	Domain	ConnectedServer: ADRoot.a1.com
7/4/2011 4:47 AM	Info	User	A1\Administrator (CN=Administrator,CN=Users,DC=a1,DC=com)
7/4/2011 4:47 AM	Info	User	A1\Guest (CN=Guest,CN=Users,DC=a1,DC=com)
7/4/2011 4:47 AM	Info	User	A1\kbtgt (CN=kbtgt,CN=Users,DC=a1,DC=com)
7/4/2011 4:47 AM	Info	User	A1\user1 (CN=user1,CN=Users,DC=a1,DC=com)
7/4/2011 4:47 AM	Info	User	A1\testuser1 (CN=testuser1\OU=TestOU,DC=a1,DC=com)
7/4/2011 4:47 AM	Info		Ending users crawl from domain: a1.com
7/4/2011 4:47 AM	Info		Ending users crawl from all forests

If you try to close this window during the crawl process, you will be informed that this will stop the current crawl.

[Go to top of section →](#)

Test Forms Based Authentication Stores Interrogation

If you have configured Forms Based Authentication (FBA) for a SharePoint Web Applications, you can use the DPChecker to test the connection to the FBA store:

1. Start the DeliverPoint Checker, and then click **Test FBA interrogation**, no other configuration is needed.

The Interrogation Report dialog box is displayed showing the progress of the crawl. The DPChecker will then connect to each Web Application and read the web.config for FBA settings.

Interrogation report			
Date	Log Type	Content Type	Message
7/4/2011 4:57 AM	Info		--- Starting FBA crawl ---
7/4/2011 4:57 AM	Info		Getting web applications to get settings from them
7/4/2011 4:58 AM	Info	WebApplication	SharePoint - 111
7/4/2011 4:58 AM	Info		Getting settings from web application: SharePoint - 111
7/4/2011 4:58 AM	Info	ConnectionString	LocalSqlServer
7/4/2011 4:58 AM	Info	WebApplication	SharePoint - 222
7/4/2011 4:58 AM	Info		Getting settings from web application: SharePoint - 222
7/4/2011 4:58 AM	Info	ConnectionString	fbacbaConnectionString
7/4/2011 4:58 AM	Info	ConnectionString	LocalSqlServer
7/4/2011 4:58 AM	Info	MembershipProv...	Default is: i
7/4/2011 4:58 AM	Info	MembershipProv...	AspNetSqlMembershipProvider
7/4/2011 4:58 AM	Info	RoleProvider	Default is: c
7/4/2011 4:58 AM	Info	RoleProvider	AspNetSqlRoleProvider
7/4/2011 4:58 AM	Info	RoleProvider	Roles enabled: true
7/4/2011 4:58 AM	Info	WebApplication	SharePoint - 80
7/4/2011 4:58 AM	Info		Getting settings from web application: SharePoint - 80
7/4/2011 4:58 AM	Info	ConnectionString	LocalSqlServer
7/4/2011 4:58 AM	Info		Starting FBA crawl from all web applications
7/4/2011 4:58 AM	Info		Configuring connection strings section
7/4/2011 4:58 AM	Info	ConnectionString	LocalSqlServer
7/4/2011 4:58 AM	Info	ConnectionString	fbacbaConnectionString
7/4/2011 4:58 AM	Info		Configuring providers
7/4/2011 4:58 AM	Info	MembershipProv...	AspNetSqlMembershipProvider
7/4/2011 4:58 AM	Info	RoleProvider	AspNetSqlRoleProvider
7/4/2011 4:58 AM	Info		Binding new settings
7/4/2011 4:58 AM	Info		Crawling users from: SharePoint - 222
7/4/2011 4:58 AM	Info	User	fUser2
7/4/2011 4:58 AM	Info	User	fUser1
7/4/2011 4:58 AM	Info		Crawling roles from: SharePoint - 222
7/4/2011 4:58 AM	Info	Group	fRole1

When a Web Application is not configured for FBA, then an error message is displayed for that Web Application.

[Go to top of section →](#)

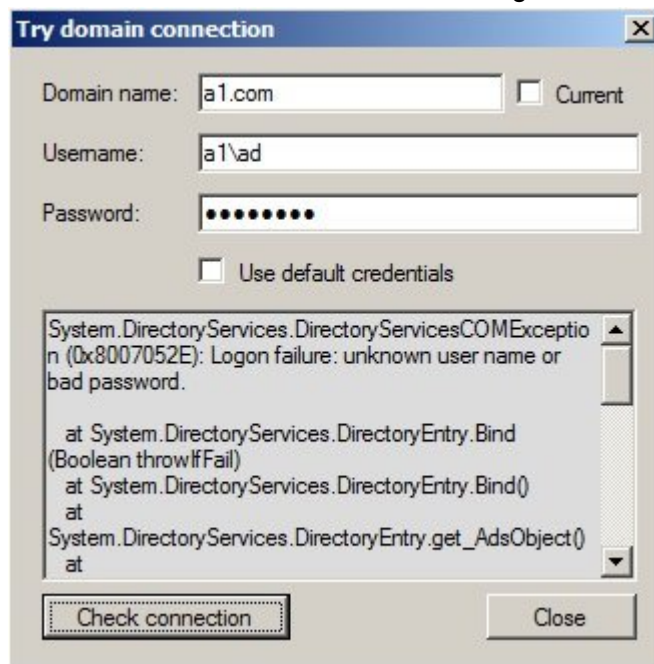
Try Domain Connections

You can use DPChecker to test connections to a specific domain, using the following steps:

1. Start the DeliverPoint Checker, and in the Forests section click **Try domain connections**.
The Try domain connection dialog box is displayed.
2. In the **Domain name** text box, type the name of the domain you wish to test or select the **Current** check box if you want to test the current domain.
3. Either:

- In the **Username** text box, type the AD username, which should be used to perform the specified forest (all its subdomains) users/groups enumeration, and in the **Password** text box, type the password.
 - Select **Use default credentials** to use current logged in user for the specified forest crawl.
3. Click **Check connection**.

When DPChecker is able to successfully connect to the domain, the word **Success** is displayed in the bottom list box, otherwise, error messages will be displayed, similar to the following screen shot.

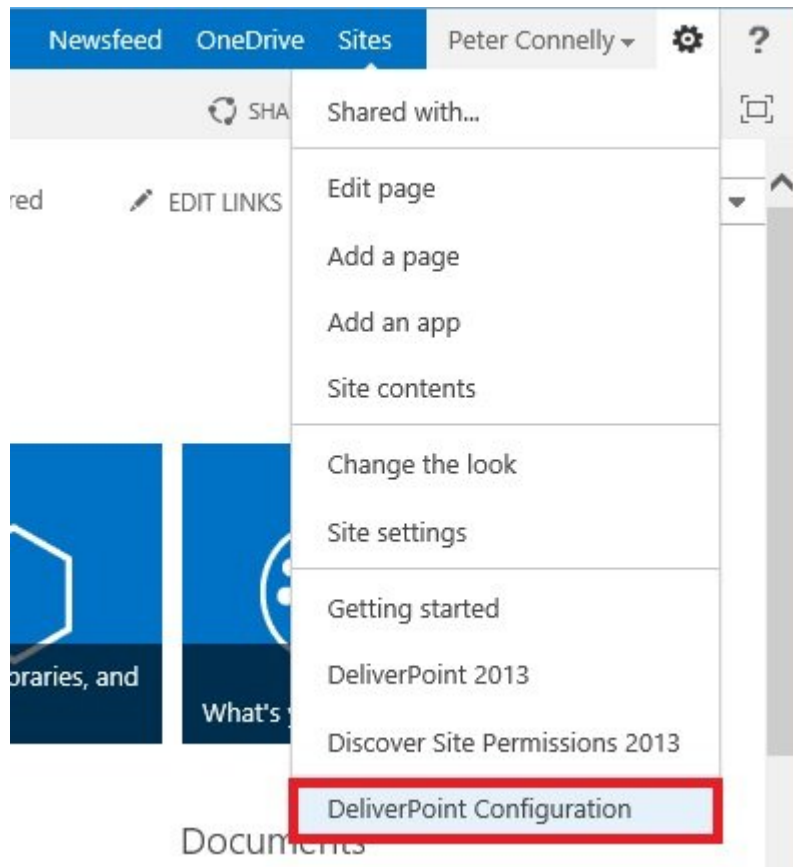


[Go to top of section →](#)

[<< How to find the DeliverPoint version](#)
[DeliverPoint Central Administration >>](#)

DeliverPoint Central Administration

There are certain DeliverPoint configuration settings that affect the whole farm and are available from the **DeliverPoint Configuration** link on the **Settings** menu on the SharePoint 2013 Central Administration web site:



* You can use the other two options on the [Settings](#) menu, to complete [permission management](#) tasks.

The **DeliverPoint Configuration** page is displayed.

[Lightning Tools](#) > DeliverPoint 2013 Configuration

DeliverPoint Configuration ⓘ

Forest Settings

Manage forests and domains registered for crawl. Add/delete new forests and domain registrations, change access credentials.



Treeview Settings

Update the settings for the DeliverPoint Treeview.



Threshold Settings

Update the DeliverPoint threshold settings - update thresholds for the size and age of web applications, wait interval after each interrogation and other settings.



Permission

Update the settings for the Permissions module. Specify the site collection administrator replacement and specify DeliverPoint operators.



TimerJob Settings

Update the settings for the DeliverPoint timer jobs. Specify the interrogations logging level, SharePoint interrogation type.



The **DeliverPoint Configuration** page contains the following options:

- [Forest Settings](#)
- [Treeview Settings](#)
- [Threshold Settings](#)
- [Permission](#)
- [TimerJob Settings](#)
- [Database Settings](#)

Forest Settings

Use this option to manage Active Directory forests and domains that you wish to crawl, together with the credentials you wish to use. The **Forest settings** page consists of one section Forest list, where you can modify the following settings:

- **Registered forest names.** This list contain all those forests that are to be interrogated when the LightningTools.DeliverPoint.AuthStoreInterrogation SharePoint time job runs. By default only one entry is listed, **Current Forest**. If you need to remove a AD forest you previously registered, select the forest and then click **Remove**. You cannot delete **Current Forest**.
- **Register new forest.** To register a new AD forest to interrogate, complete the following:
 - In the **Forest name** text box, type the forest name – you must enter a DNS name.
 - In the **Account name** text box, type the AD username, which should be used to perform the specified forest (all it subdomains) users/groups enumeration.
 - In the **Account Password** text box, type the password.
 - Click **Add**.
- **Domain Exclusions.** Use this list box to type all domain names that should be excluded during authentication interrogation. Valid values are domain names and NetBIOS names.

Forest settings ⓘ

Forest list

Add/remove forests to crawl from. Use access credentials for each forest registration. You cannot remove the 'Current Forest' entry. Use Excluded Domains list to exclude domains from DeliverPoint interrogation.

Registered forest names

Current Forest

Remove selected forest from the list

Remove

Register new forest

Forest name

Account name

Account Password

Add

Domain Exclusions

Enter excluded domain names separated with semicolons

OK

Cancel

[Go to top of section →](#)

Treeview Settings

Use this option to configure the DeliverPoint treeview that is displayed on the DeliverPoint dashboard. The DeliverPoint treeview settings page consists of four sections:

- **Display Segments.** In the **Segments** text box, type the maximum number of tree nodes to display at the Site Collection and Site level. When the number of objects exceeds this level, the treeview is segmented. The default value is 100.

- **View Restriction.** You can select one of two options that allows you to restrict the treeview so that it is only displayed for Site Collection Administrators:
 - **Yes, restrict.**
 - **No, not restricted** (default).
- **Hide not accessible tree nodes.** Use this to hides high level tree nodes if current user has no permissions over the specified node scope. If you display the high level nodes, this can cause performance issues if there are large amount of sites/webs in crawling scope. You can select on of the following two options:
 - **Show.**
 - **Hide (recommended).** (default)
- **Show lists/libraries in treeview and in report.** Use this to manages the visibility of lists and libraries in the treeview. By default no option is selected.
 - **Show Lists and Libraries In Report.**

DeliverPoint Treeview settings ⓘ

Display Segments

Please enter the maximum number of tree nodes to display at any level. A number that is too large will degrade performance when expanding the nodes.

Segments:

View Restriction

Restrict the tree view to show sites to Site Collection Administrators only.

Restriction:

- ☐ Yes, restricted
☒ No, not restricted

Hide not accessible tree nodes

Hides high level tree nodes if current user has no permissions over the specified node scope. Can cause performance issues if there are large amount of sites/webs in crawling scope.

- ☐ Show
☒ Hide (recommended)

Show lists/libraries in treeview and in report

Manages visibility of lists and libraries in the treeview.

☐ Show Lists and Libraries In Report

OK

Cancel

[Go to top of section →](#)

Threshold Settings

Use this option to update the DeliverPoint threshold settings, which are used when displaying the [Properties](#) usage report in the [DeliverPoint dashboard](#) results pane. The DeliverPoint Threshold Settings page contains the following sections:

- **Wait Threshold.** The interval, in milliseconds, the SharePoint Interrogation timer jobs waits before it requests the next site (web). The default is 100 milliseconds.

- **Web Application Thresholds.** Segments Web Applications into Small, Large, New, and Old thresholds. Small and Large sizes are in MB. The defaults are 1, 3 MB, respectively. New and Old are specified in days. The defaults are 10 and 100 days, respectively.
- **Managed Path Thresholds.** Segments Managed Paths into Small, Large, New, and Old thresholds. Small and Large sizes are in MB. The defaults are 1, 3 MB, respectively. New and Old are specified in days. The defaults are 10 and 100 days, respectively.
- **Site Collection Thresholds.** Segments Site Collections into Small, Large, New, and Old thresholds. Small and Large sizes are in MB. The defaults are 1, 3 MB, respectively. New and Old are specified in days. The defaults are 10 and 100 days, respectively.
- **Site Thresholds.** Segments Sites into Small, Large, New, and Old thresholds. Small and Large sizes are in MB. The defaults are 1, 3 MB, respectively. New and Old are specified in days. The defaults are 10 and 100 days, respectively.
- **List Thresholds.** Segments Lists into Small, Large, New, and Old thresholds. Small and Large sizes are in MB. The defaults are 1, 3 MB, respectively. New and Old are specified in days. The defaults are 10 and 100 days, respectively.

DeliverPoint Threshold settings ⓘ

Wait Threshold

Enter the interval that the interrogation process waits after each web.

Wait Threshold:

Web Application Thresholds

Enter the thresholds for the size and age of web applications.

Small (MB):

Large (MB):

New (days):

Old (days):

Managed Path Thresholds

Enter the thresholds for the size and age of managed paths.

Small (MB):

Large (MB):

New (days):

Old (days):

Site Collection Thresholds

Enter the thresholds for the size and age of site collections.

Small (MB):

[Go to top of section →](#)

Permissions

Use this option to update the settings for the permissions module. The **DeliverPoint Permission settings** page contain two sections:

- **Replacement User.** Use the **user account** people picker to specify the account to be used to replace the last site collection administrator on a site collection when DeliverPoint is removing the last site collection administrator via a “Delete” or “Dead Account Removal” operation. If this field is left blank, the account of the user using the DeliverPoint operation will become the new, last site collection administrator for the site collection(s) in question.
- **Permissions module operators.** Use the **Operator accounts** people picker to specify one or more users. Such users can manage permissions on any site regardless of their permission on a SharePoint object. The user(s) entered in this text box have unrestricted access when using DeliverPoint, however, these user(s) are not given SharePoint access to any content from this designation. Any Operator must have access to at least one SharePoint site to use DeliverPoint.
- **Permissions module auditors.** Use the **Auditor accounts** people picker to specific one or more users. These users are allowed read only permissions to run permission reports via DeliverPoint. regardless of their permissions on SharePoint objects.

DeliverPoint Permissions settings ⓘ

Replacement User

All site collections must have at least one administrator. In the event that a DeliverPoint Delete operation will remove the final site collection administrator, the Replacement User account will become the site collection administrator.

User account



Permissions module operators

Selected users will be allowed to do all permission management operations via DeliverPoint regardless of their permissions.

Operator accounts:



Permissions module auditors

Selected users will be allowed to do all read only permission management operations via DeliverPoint regardless of their permissions.

Auditor accounts:



OK

Cancel

[Go to top of section →](#)

TimerJob Settings

Use this option to configure the three timer jobs. The **DeliverPoint timer job settings** page contains the following sections:

- **SharePoint crawl method.** Use to specify the SharePoint crawler method – **Full** or **Incremental**. Incremental crawl is recommended, if you have a large SharePoint farm. The Incremental option is the default select option when you first install DeliverPoint. As you can only use incremental crawls once a full crawl has successfully completed, you must [first select Full and run the SharePoint timer job](#) before reselecting Incremental. Crawling SharePoint content can take a [considerable time](#).
- **Logging level.** Use to control logging level for all timer jobs. You can select one of the following two logging levels:
 - **Deep:** log info, warning and error messages.
 - **Errors.** log only error messages. (default)
- **Exclusions List/Library Types.** Use to select list types to be excluded from permission scans. By default lists created from any list type will be crawled. You can select one or more of the following list types: NoListTemplate, GenericList, DocumentLibrary, Survey, Links, Announcements, Contacts, Events, Tasks, DiscussionBoard, PictureLibrary, DataSources, WebTemplateCatalog, UserInformation, WebPartCatalog, ListTemplateCatalog, XMLForm, MasterPageCatalog, NoCodeWorkflows, WorkflowProcess, WebPageLibrary, CustomGrid, SolutionCatalog, NoCodePublic, ThemeCatalog, DataConnectionLibrary, WorkflowHistory, GanttTasks, Meetings, Agenda, MeetingUser, Decision, MeetingObjective, Textbox, ThingsToBring, HomePageLibrary, Posts, Comments, Categories, Facility, Whereabouts, CallTrack, Circulation, Timecard, Holidays, IMEDic, ExternalList, IssueTracking, AdminTasks, HealthRules, HealthReports, InvalidTypes.
- **Report Generation Settings** Use this section to specify the default folder and the file name pattern for the [scheduled permission reports](#).

DeliverPoint timer job settings ⓘ

SharePoint crawl method

Specify SharePoint crawler method - full or incremental. Incremental crawl is recommended, if SharePoint Farm is big.

- ☐ Full: Deletes old crawled data and performs new full SharePoint crawl
- ☒ Incremental: Performs partial crawl over the changed content only

Logging level

Control logging level for all timer jobs.

Logging Level:

- ☐ Deep: log info, warning and error messages
- ☒ Errors: log only error messages

Exclusions List/Library Types

Mark list types to be excluded from permission scans

Exclude List Types:

- ☐ NoListTemplate
- ☐ GenericList
- ☐ DocumentLibrary
- ☐ Survey
- ☐ Links
- ☐ Announcements
- ☐ Contacts
- ☐ Events
- ☐ Tasks
- ☐ DiscussionBoard
- ☐ PictureLibrary
- ☐ DataSources
- ☐ WebTemplateCatalog

[Go to top of section →](#)

Database Settings:

When you [install DeliverPoint](#), you are required to provide details so that a DeliverPoint database is created. On the **DeliverPoint Database Settings** page, the information that you provided when the DeliverPoint Configuration Wizard was run are used to pre-populated fields on this page.

Note: These settings may be altered in the event of a DeliverPoint database migration. The **DeliverPoint Database Settings** page contains the following sections:

- DeliverPoint Database. This section consists of two text boxes:

- **Server:** The server NETBIOS name of the SQL Server, where the DeliverPoint database is hosted.
- **Database:** The name of the DeliverPoint database.
- DeliverPoint DB Account. This section contains two text boxes:
 - **DB Account Name:** The impersonation account, also known as the DeliverPoint Service Account, used to access the DeliverPoint database and interrogate the SharePoint databases via the SharePoint Object Model (OM). The service account requirements are listed in the section: [Deploying DeliverPoint](#).
 - **DB Account Password:** The password for the DeliverPoint Service Account.

DeliverPoint Database Settings ⓘ

DeliverPoint Database

Please enter the name of the server (and instance if applicable) and database.

Server:

Enter the server NETBIOS name. If the database is not in the default instance, enter the information in the format SERVER\INSTANCE.

Database:

DeliverPoint DB Account

Specify a user account to be used by the application to connect to Deliverpoint DB (in format DOMAIN\username)

DB Account Name:



DB Account Password:

[Go to top of section →](#)

[<< DeliverPoint Checker](#)


[Restricting access to DeliverPoint >>](#)

Restricting access to DeliverPoint

DeliverPoint allows you to easily [restrict the tree view](#) on the [Farm](#) and [Account](#) centric views, so that it is only displayed for Site Collection Administrators.

You can use the information on this page if you want to restrict ALL references to DeliverPoint 2013 in the browser User Interface to Site Collection Administrators and above.

By default DeliverPoint is available on the following User Interface objects:

- [Settings](#)  menu.
- Site Settings page for each site.
- [DeliverPoint Ribbon tab](#), for example, when displaying a view of a list or library, edit properties page for a list item or file, and view properties page for a list item or file.
- [List Item Menu](#) on list items or files.

The DeliverPoint links are configured using a Ribbon XML elements file, which contains one or more < CustomAction > tags as described below:

- Two < CustomAction > tags to define the two DeliverPoint options on the Site Actions menu, known as Microsoft.SharePoint.StandardMenu.
- Two < CustomAction > tags to define the two DeliverPoint options on the Site Settings page, known as Microsoft.SharePoint.SiteSettings.
- One < CustomAction > tag to define the DeliverPoint link on the List Item Menu, also known as EditControlBlock.
- One < CustomAction > tag to place the Discover Permissions option on the Ribbon on pages that display or allow you to edit item properties, known as DisplayFormToolbar.
- 39 < CustomAction> tag to configure the DeliverPoint tab for each list type, known as CommandUI.Ribbon.

You will need to amend each of the < CustomAction > tags in the DeliverPoint Ribbon XML elements file on every SharePoint Web-front end, if you want the DeliverPoint links to appear for only Site Collection Administrators or above, using the steps described below.




In a production environment you will need to raise a change request to complete all the steps detailed on this page. Also, as the procedure requires an IISRESET, you will probably not be allowed to complete the task during production hours.

Note: If an account, *DOM\user1*, is a site collection administrator and is also configured as a [system account](#), the account is not identified as site collection administrator. When an account operates as the system account, it runs using the account *SHAREPOINT\system*. The *SHAREPOINT\system* account is used when a user is logged in as *DOM\user1*. The work around in this scenario, is to either remove the system designation for *DOM\user1* – or – designate *SHAREPOINT\system* as a site collection administrator.



Creating a new web application with a new application pool will cause the DeliverPoint User Interface feature to be re-deployed. Any customizations you have made will need to be reapplied once the web application is created. We would like to send a special thanks to the HNTB team for pointing this out to us.

To restrict access to DeliverPoint use the following steps:

1. In the browser, after installing DeliverPoint 2013, navigate to SharePoint 2013 Central Administration web site.
2. Click **Settings** , and then click [DeliverPoint Configuration](#).
3. Click **Treeview Settings**.
4. In the **View Restrictions** section, select **Yes**.
5. Click **OK**.
6. On each SharePoint server that is running the [Microsoft SharePoint Foundation Web Application service](#), navigate to folder:
C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions
\15\TEMPLATE\FEATURES\LightningTools.DeliverPoint.Web.UI_DP13UI\DP13UI-Links
7. First take a copy of the file, **Elements.xml**, so you can quickly revert to a working copy of the file if you accidentally incorrectly modify the file, so that the DeliverPoint User Interface object no longer work.
8. Edit the **Elements.xml** file in Visual Studio or Notepad.
9. Insert an additional line after line 10,
Title="\$Resources:LightningTools.DeliverPoint.Web.UI,DPSiteActionsDeliverPointTitle;" and type:
RequireSiteAdministrator="TRUE"
This will remove the *DeliverPoint 2013* option from the *Settings* menu.
10. If you would also like to remove the *Discover Site Permissions 2013* from the *Settings* menu, then after line 21, *Title="\$Resources:LightningTools.DeliverPoint.Web.UI,DPSiteActionsDeliverPointTitle;"*,

type on a new line:

RequireSiteAdministrator="TRUE"

11. Repeat similar configuration for the *EditControlBlock*, *DisplayFormToolbar* and *Microsoft.SharePoint.SiteSettings* < CustomAction > tags.

12. Then from EVERY
 < CustomAction >

...

 < / CustomAction >

section, if **Rights="EnumeratePermissions"** is specified, delete it.

13. Save the file.
14. Use IISReset to stop and restart the entire IIS web server on each SharePoint server where you have made the amendment.

References

- [Microsoft SharePoint Team Blog: Enabling a Button on the Ribbon Based on Selection](#)
- [Customizing the Ribbon blog series by Chris O'Brien](#)
- [SharePoint Conference: Session SPC402 Ribbon Development and Extensibility](#)

[<< DeliverPoint Central Administration](#)

[Powershell Commands >>](#)

Powershell Commands

DeliverPoint Cmdlets

DeliverPoint operations can be performed also via Powershell.



It is extremely important to make sure that the DeliverPoint Crawls are up-to-date prior to performing any cmdlets that affect permissions.

The following commands are available:

Copy Permissions

Copy-FarmPermissions -Url -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -ExcludeLists -
ExcludelItems -SupportRollback -ContextUser

Copy-WebAppPermissions -Url -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -ExcludeLists -
ExcludelItems -SupportRollback -ContextUser

Copy-ManagedPathPermissions -Url -Prefix -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -
ExcludeLists -ExcludelItems -SupportRollback -ContextUser

Copy-SitePermissions -Url -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -ExcludeLists -
ExcludelItems -SupportRollback -ContextUser

Copy-WebPermissions -Url -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -ExcludeLists -
ExcludelItems -IncludeSubWebs -SupportRollback -ContextUser

Copy-ListPermissions -Url -ListTitle -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -ExcludeLists -
ExcludelItems -SupportRollback -ContextUser

Copy-ItemPermissions -Url -ListTitle -ItemId -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -
ExcludeLists -ExcludelItems -SupportRollback -ContextUser

The parameters are described below:

1. Url – is mandatory and specifies URL of the operation scope. For farm scope it contains URL of any web application of that farm. And for managed path scope it contains URL of any web application containing the managed path.
2. From – is mandatory and specifies SP group/user, from which permissions must be copied. If FromGroup paramatere is specified, than value of From parameter is treated as SP group, otherwise as SP user.
3. ToUsers – comma separated list of SP user login names, to which permissions must be copied. At least one parameter from ToUsers/ToGroups must be specified.
4. ToGroups – comma separated list of SP group names, to which permissions must be copied. At least one parameter from ToUsers/ToGroups must be specified.
5. IncludeAlerts – if present means, that SP alerts also must be coped.
6. ExcludeLists – if present means, that unique lists of processed webs must be excluded from copying permissions.
7. ExcludelItems – if present means, that unique items of processed lists must be excluded from copying permissions.
8. IncludeSubWebs – used only for web scope and if present means, that unique sub webs of the web also be take part into copying of permissions.
9. SupportRollback – can be None/On/Off (if not present, than None). Specifies whether created job will support or not support rollback (On – support, Off – not support, None – use default value specified from DP central administration settings).
10. ContextUser – login name of user, in context of which copy permission must be performed (if not specified job will be executed in system account context).
11. Prefix – used for specifying managed path prefix (used for managed path scope only and is mandatory)
12. ListTitle – used for List/Item scopes only in cases when user wants to specify list by title (in that case Url parameter can be parent web URL).
13. ItemId – used for item scopes only in cases when user wants to specify item by id (in that case Url parameter can be parent list URL of parent web URL if ListTitle parameter also has been specified).

Transfer Permissions

Transfer-FarmPermissions -Url -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -ExcludeLists - ExcludelItems -SupportRollback -ContextUser

Transfer-WebAppPermissions -Url -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -ExcludeLists - ExcludelItems -SupportRollback -ContextUser

Transfer-ManagedPathPermissions -Url -Prefix -From -ToUsers -ToGroups -FromGroup -IncludeAlerts - ExcludeLists -ExcludelItems -SupportRollback -ContextUser

Transfer-SitePermissions -Url -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -ExcludeLists -
ExcludelItems -SupportRollback -ContextUser

Transfer-WebPermissions -Url -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -ExcludeLists -
ExcludelItems -IncludeSubWebs -SupportRollback -ContextUser

Transfer-ListPermissions -Url -ListTitle -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -ExcludeLists
-ExcludelItems -SupportRollback -ContextUser

Transfer-ItemPermissions -Url -ListTitle -ItemId -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -
ExcludeLists -ExcludelItems -SupportRollback -ContextUser

Parameters has just the same meaning as from first group of commands.

Replace Permissions

Replace-FarmPermissions -Url -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -ExcludeLists -
ExcludelItems -SupportRollback -ContextUser

Replace-WebAppPermissions -Url -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -ExcludeLists -
ExcludelItems -SupportRollback -ContextUser

Replace-ManagedPathPermissions -Url -Prefix -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -
ExcludeLists -ExcludelItems -SupportRollback -ContextUser

Replace-SitePermissions -Url -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -ExcludeLists -
ExcludelItems -SupportRollback -ContextUser

Replace-WebPermissions -Url -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -ExcludeLists -
ExcludelItems -IncludeSubWebs -SupportRollback -ContextUser

Replace-ListPermissions -Url -ListTitle -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -ExcludeLists
-ExcludelItems -SupportRollback -ContextUser

Replace-ItemPermissions -Url -ListTitle -ItemId -From -ToUsers -ToGroups -FromGroup -IncludeAlerts -
ExcludeLists -ExcludelItems -SupportRollback -ContextUser

Parameters has just the same meaning as from first group of commands.

Delete Permissions

Delete-FarmPermissions -Url -FromUsers -FromGroups -IncludeAlerts -ExcludeLists -Excludeltems - SupportRollback -ContextUser

Delete-WebAppPermissions -Url -FromUsers -FromGroups -IncludeAlerts -ExcludeLists -Excludeltems - SupportRollback -ContextUser

Delete-ManagedPathPermissions -Url -Prefix -FromUsers -FromGroups -IncludeAlerts -ExcludeLists -Excludeltems -SupportRollback -ContextUser

Delete-SitePermissions -Url -FromUsers – FromGroups -IncludeAlerts -ExcludeLists -Excludeltems - SupportRollback -ContextUser

Delete-WebPermissions -Url -FromUsers – FromGroups -IncludeAlerts -ExcludeLists -Excludeltems - IncludeSubWebs -SupportRollback -ContextUser

Delete-ListPermissions -Url -ListTitle -FromUsers -FromGroups -IncludeAlerts -ExcludeLists -Excludeltems - SupportRollback -ContextUser

Delete-ItemPermissions -Url -ListTitle -ItemId -FromUsers -FromGroups -IncludeAlerts -ExcludeLists -Excludeltems -SupportRollback -ContextUser

Parameters has the following meaning:

1. FromUsers – comma separated list of SP user login names, from which permissions must be deleted. At least one parameter from FromUsers/FromGroups must be specified.
2. FromGroups – comma separated list of SP group names, from which permissions must be deleted. At least one parameter from FromUsers/FromGroups must be specified.
3. Other parameters has the same meaning as for first group of commands.

Grant Permissions

Grant-FarmPermissions -Url -ToUsers -ToGroups -Permissions -Groups -ProcessLists -Processltems - GrantDuration -SupportRollback -ContextUser

Grant-WebAppPermissions -Url -ToUsers -ToGroups -Permissions -Groups -ProcessLists -Processltems - GrantDuration -SupportRollback -ContextUser

Grant-ManagedPathPermissions -Url -Prefix -ToUsers -ToGroups -Permissions -Groups -ProcessLists - Processltems -GrantDuration -SupportRollback -ContextUser

Grant-SitePermissions -Url -ToUsers -ToGroups -Permissions -Groups -ProcessLists -ProcessItems -
GrantDuration -SupportRollback -ContextUser

Grant-WebPermissions -Url -ToUsers -ToGroups -Permissions -Groups -ProcessSubWebs -ProcessLists -
ProcessItems -GrantDuration -SupportRollback -ContextUser

Grant-ListPermissions -Url -ListTitle -ToUsers -ToGroups -Permissions -Groups -ProcessLists -
ProcessItems -GrantDuration -SupportRollback -ContextUser

Grant-ItemPermissions -Url -ListTitle -ItemId -ToUsers -ToGroups -Permissions -Groups -ProcessLists -
ProcessItems -GrantDuration -SupportRollback -ContextUser

Parameters has the following meaning:

1. ToUsers – comma separated list of SP user login names, to which permissions must be granted. At least one parameter from ToUsers/ToGroups must be specified.
2. ToGroups – comma separated list of SP group names, to which permissions must be granted. At least one parameter from ToUsers/ToGroups must be specified.
3. Permissions – comma separated of permission level, which must be granted to users/groups specified by parameters ToUsers/ToGroups.
4. Groups – comma separated list of SP group names, to which users specified by parameter ToUsers must be added.
5. ProcessSubWebs – if present means, that unique sub webs of web also must be processed.
6. ProcessLists – if present means, that unique lists of processed lists also must be processed.
7. ProcessItems – if present means, that unique items of processed lists also must be processed.
8. GrantDuration – contains duration in minutes after which granted permissions will be automatically revoked. If not specified (or negative) than no automatic revoke will be done.
9. Other parameters has the same meaning as for first group of commands.

Revoke Permissions

Revoke-FarmPermissions -Url -FromUsers -FromGroups -Permissions -Groups -ProcessLists -ProcessItems
-SupportRollback -ContextUser

Revoke-WebAppPermissions -Url -FromUsers -FromGroups -Permissions -Groups -ProcessLists -
ProcessItems -SupportRollback -ContextUser

Revoke-ManagedPathPermissions -Url -Prefix -FromUsers -FromGroups -Permissions -Groups -
ProcessLists -ProcessItems -SupportRollback -ContextUser

Revoke-SitePermissions -Url -FromUsers -FromGroups -Permissions -Groups -ProcessLists -ProcessItems -SupportRollback -ContextUser

Revoke-WebPermissions -Url -FromUsers -FromGroups -Permissions -Groups -ProcessSubWebs -ProcessLists -ProcessItems -SupportRollback -ContextUser

Revoke-ListPermissions -Url -ListTitle -FromUsers -FromGroups -Permissions -Groups -ProcessLists -ProcessItems -SupportRollback -ContextUser

Revoke-ItemPermissions -Url -ListTitle -ItemId -FromUsers -FromGroups -Permissions -Groups -ProcessLists -ProcessItems -SupportRollback -ContextUser

Parameters has the following meaning:

1. FromUsers – comma separated list of SP user login names, from which permissions must be revoked. At least one parameter from FromUsers/FromGroups must be specified.
2. FromGroups – comma separated list of SP group names, from which permissions must be revoked. At least one parameter from FromUsers/FromGroups must be specified.
3. Permissions – comma separated of permission level, which must be revoked from users/groups specified by parameters FromUsers/FromGroups.
4. Groups – comma separated list of SP group names, from which users specified by parameter ToUsers must be removed.
5. ProcessSubWebs – if present means, that unique sub webs of web also must be processed.
6. ProcessLists – if present means, that unique lists of processed lists also must be processed.
7. ProcessItems – if present means, that unique items of processed lists also must be processed.
8. GrantDuration – contains duration in minutes after which granted permissions will be automatically revoked. If not specified (or negative) than no automatic revoke will be done.
9. Other parameters has the same meaning as for first group of commands.

Dead Account Removal

Delete-FarmDeadAccounts -Url -DeadAccounts -ContextUser -AllowDisabled

Delete-ManagedPathDeadAccounts -Url -Prefix -DeadAccounts -ContextUser -AllowDisabled

Delete-WebAppDeadAccounts -Url -DeadAccounts -ContextUser -AllowDisabled

Delete-SiteDeadAccounts -Url -DeadAccounts -ContextUser -AllowDisabled

Parameters has the following meaning:

1. DeadAccounts – comma separated list of dead account names to be deleted. If not specified or empty, than all dead accounts going to be deleted.

2. AllowDisabled – On or Off (If not specified than Off). Specifies whether disabled dead accounts also must be deleted or not (dead accounts are of two types: first type users appear because of not existence of appropriate users in AD and second type users appear because of disabling appropriate user in AD).
3. Other parameters has the same meaning as for first group of commands.

Clone Permissions

Clone-WebPermissions -SourceUrl -TargetUrls -CloneGroups -CloneRoleDefinitions -SupportRollback -ContextUser

Clone-ListPermissions -SourceUrl -TargetUrls -CloneGroups -CloneRoleDefinitions -SupportRollback -ContextUser

Clone-ItemPermissions -SourceUrl -TargetUrls -CloneGroups -CloneRoleDefinitions -SupportRollback -ContextUser

Parameters has the following meaning:

1. SourceUrl – is Url of source scope.
2. TargetUrls – is comma separated list of target scope Urls.
3. CloneGroups – if present means, that missing SP groups will also be cloned to the target web(s).
4. CloneRoleDefinitions – if present means, that missing role definitions will also be cloned to the target web(s).
5. Other parameters has the same meaning as for first group of commands.

Exclude Web Applications

Get-DPWebAppExclusions

Add-DPWebAppExclusions -WebAppUrl -Id

Remove-DPWebAppExclusions -WebAppUrl -Id

First command is for showing all excluded web application from SharePoint crawl. Second command is for excluding specified web application from SharePoint crawl. Third command is for removing specified web application from SharePoint crawl exclusion list. Parameters has the following meaning:

1. WebAppUrl – Url of provided web application (if it provided by Url).
2. Id – Id of provided web application (if it provided by id).

Checking the DeliverPoint Versions

Get-DPVersion

Displaying Job Information

Get-DPJobs -JobId -ContextUser

Parameters has the following meaning:

1. JobId – specified id of the DP job, information about which must be shown. If not specified, than list of all DP jobs will be shown.
2. ContextUser – login name of user, in context of which DP jobs must be retrieved (i.e. only jobs accessible by provided user will be shown). If not specified, than all jobs are treated to be accessible.

Modifying Settings

Set-DPCommonSettings -RenderUrlsInExportedDiscoverPermissions

Parameters has the following meaning:

1. RenderUrlsInExportedDiscoverPermissions – On/Off or None. On values means, that Urls must be rendered in discover permissions report. Off value, means that Urls must not be rendered in discover permissions report. Missing or None value means, that appropriate setting will not be changed.

Setting DeliverPoint Jobs

Set-DPJobsSettings -ForceBreakScopePermissions -ReplacePermissionsOperation -
JobsSupportRollbackByDefault

Parameters has the following meaning:


1. ForceBreakScopePermissions – On/Off or None. On value means turning on ability of forcing breaking scope permissions (when needed) during execution of DP jobs. Off value means turning off the mentioned ability. None or missing value means not modifying the mentioned ability.
2. ReplacePermissionsOperation – On/Off or None. On value means showing replace permissions operation related commands in DeliverPoint UI. Off value means hiding replace permissions operation related commands from DeliverPoint UI. None or missing value means not modifying the mentioned visibility.
3. JobsSupportRollbackByDefault – On/Off or None. On value means, that by default (i.e. when user hasn't specified it explicitly) DP jobs must support rollback. Off value means, that by default DP jobs must not support rollback. None or missing value means, that mentioned default behavior will not be modified.

Permission Management


[DeliverPoint 2013](#) allows a variety of users: [DeliverPoint permission operators](#), site collection administrators, site owners, power users, and end users; to manage SharePoint permissions in Microsoft® SharePoint® Server 2013 or Microsoft® SharePoint Foundation 2013 on-premises deployments.

✿ If you are new to managing permissions in SharePoint 2013, then you will find some useful links in the [References](#) section at the bottom of this page.

Users can use DeliverPoint to manage permissions from:

- The [Settings](#)  menu, to display the [DeliverPoint dashboard](#), or to run a Discover Site Permissions report.
- DeliverPoint Ribbon tab, for example, on lists and libraries, you can use the Ribbon to initiate the [Discover List Permissions](#) and discover [Unique Items](#) permissions commands.
- List Item Menu on folders, list items and files, which, for example, you can use to initiate the [Discover Items Permissions](#) action.

! If you are using a trial version of DeliverPoint, and your trial period has expired, then when you try to display the DeliverPoint dashboard, a message is displayed in the results pane: **Trial period for product DeliverPoint 2013 has been expired. Activate** Click **Activate** to display the [Licensing of Product 'DeliverPoint 2013'](#) page.

DeliverPoint allows you to manage permissions at the [account](#), farm, Web Application, site collection, site, list, folder and list item levels. To manage account permissions or permissions at a web application, site collection or site level, you use the [DeliverPoint dashboard](#). You can also use the *Discover Site Permissions* link from the Settings  menu to manage permissions at a site level. By default to manage list, folder or item permissions, navigate to the list and use the DeliverPoint Ribbon. Lists and folders permissions can also be managed using the [DeliverPoint dashboard](#) when the **Show Lists and Libraries in Reports** checkbox is selected on the [DeliverPoint Treeview settings](#) page.

For example, when using the [DeliverPoint dashboard](#), where you can switch between an [Account](#) or [Farm](#) centric view, select one or more checkbox to the left of a SharePoint object in the tree view, which activates the **Commands** Ribbon and then click the required command.

SharePoint Newsfeed OneDrive Sites Brett ?

BROWSE VIEW **COMMANDS** REPORT

SHARE FOLLOW

Common

Discover Permissions Permission Inheritance Properties Open

Account Management

Copy Permissions Grant Permissions Transfer Permissions Delete Permissions Dead Accounts

Site Management

Compare Permissions Copy Site Permissions Unique Lists

List Management

Copy List Permissions View Folders

Copy an account's permissions to another account

Aggregate Data

	New	Aging	Old	Empty	Small	Medium	Large
Managed Paths (1)	0	0	1	0	0	0	1
Site Collections (8)	0	0	8	0	0	5	3
Sites (35)	0	1	34	0	24	6	5
Lists (384)	0	17	367	16	359	7	2

The DeliverPoint command you choose affect all permissions for the targeted account in scope. For example, when you select [Copy Permissions](#) at the Managed Path level. Since all site collections within the [Managed Path](#) are part of the inheritance chain, they are said to be in scope. Site collections that exist under other Managed Paths would not be in scope because they are not part of the selected Managed Path's inheritance chain.

It is important to know which objects are in scope for every command you execute using DeliverPoint. For example, if you select the [Delete Permissions](#) command at the Farm level, then all Web Applications, Managed Paths, site collections, sites (webs), lists, list items and folders are in scope for this action. Be sure to target the execution of permissions at the intended level of inheritance so you don't change permissions for a user on the wrong or unintended objects.

- ✿ **Note** DeliverPoint is [security trimmed](#) so that users can only see information and perform DeliverPoint commands within their native scope of authority that is defined within SharePoint. That being said, it is still important to be certain that you target the desired scope in which to perform a DeliverPoint command so that unwanted changes do not occur. The [Copy](#), [Delete](#), and [Transfer Permissions](#) commands are effective on the following objects:
- * Farm
 - * Web Application
 - * Managed paths
 - * Site collections
 - * Sites (webs)

- * Lists
- * List items and folders.

References

- [Introduction: Control user access with permissions](#)
- [Video: Understanding permissions in SharePoint](#)
- [Permissions planning for sites and content in SharePoint 2013](#)
- [Plan your permissions strategy](#)
- [Governance: Permission Management](#)

[Security Trimming >>](#)

Security Trimming

[DeliverPoint 2013](#) is security trimmed; meaning, if a user can complete a security-related operation with Microsoft® SharePoint® objects using the browser, the same user is allowed to complete the identical action using DeliverPoint. When a user is a site collection administrator, they will be able to perform all security-related operations on the particular site collection for which they are the site collection administrator. When a user has full control on two sites within a site collection and they perform an security-related operation at the site collection level, the operation will only modify the sites or the content within those two sites where the user has the required permission.

DeliverPoint uses SharePoint® to determine the effective permissions of the user, based on the current site context where the user has accessed DeliverPoint. When a user accesses DeliverPoint through a site in a specific [zone](#), that same zone is used to determine effective permissions for the user on the other [web applications](#) listed in the DeliverPoint tree view.

DeliverPoint not only takes note of permissions that users may set at site collection, site, list / library, folder, item, file levels, but also uses [user policies](#) configured at the web application level. When a user policy is configured for a web application, SharePoint enforces permissions on all content within the web application, thereby enabling an organization to set security policies for users at the web application level. The permissions configured in a user policy override all other security settings that are configured for sites and content. You can configure a user policy based on users or user groups in Active Directory (AD), but not SharePoint groups. A user policy can be defined for any web application in general (all zones) or for a specific zone.

For example:

- Web Application 1
 - (A permission policy for Zone 2 does not exist)
- Web Application 2
 - (A permission policy for Zone 2 DOES exist)
- Web Application 3
 - (A permission policy for Zone 2 DOES exist)

When the user accesses a site via a URL bound to *Zone 2* on *Web Application 2* and then accesses DeliverPoint. If a request is made to view or manage permissions on the other two web applications, SharePoint uses the current user's zone when resolving any DeliverPoint request made on behalf of the user. In this scenario, when a user accesses:

- *Web Application 1*, since a permission policy for *Zone 2* does not exist, then SharePoint applies any **All zones** user policies or the **Default** zone user policy.
- *Web Application 2*, since a policy for *Zone 2* DOES exist, then that policy is applied to the request.



To restrict DeliverPoint access to site collection administrators only, see [Restricting access to DeliverPoint](#).


References

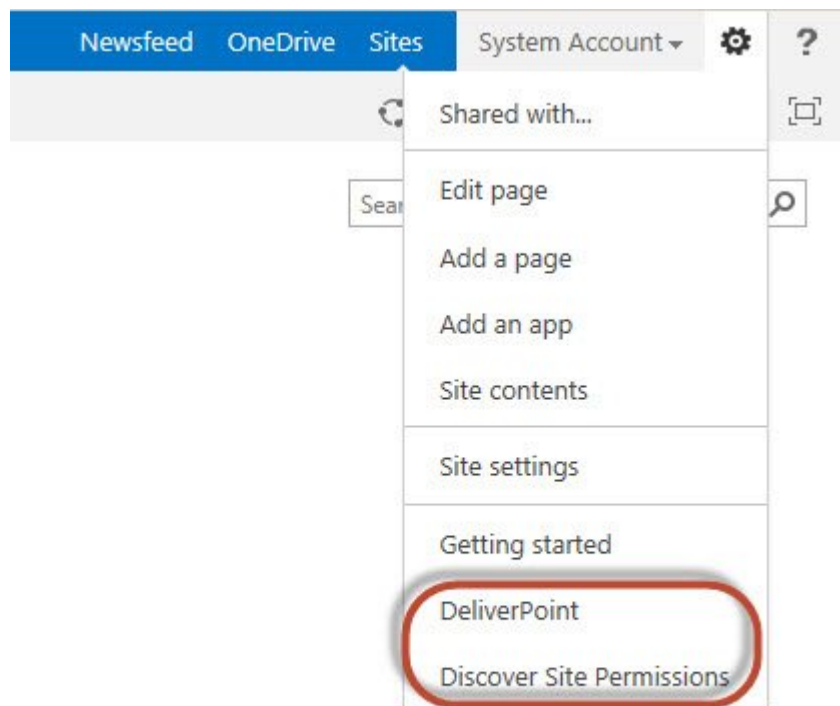
- [Plan for user authentication methods in SharePoint 2013: planning zones for web applications](#)
- [Web applications management in SharePoint Server 2013](#)
- [Manage permission policies for a web application in SharePoint 2013](#)

[<< Permission Management](#)

[DeliverPoint Settings options >>](#)

DeliverPoint Settings options

To start using DeliverPoint, navigate to a SharePoint site and then to a list or library or click **Settings** , where you will see two [DeliverPoint options](#). These two options are also available on the **Site Settings** page under **LightningTools DeliverPoint** and are therefore available on sites where the *Settings* menu is not available.



Note: Once DeliverPoint is installed there is a [DeliverPoint Ribbon](#) tab on lists and libraries, and a [List Item Menu](#) option.

✿ The DeliverPoint options on the **Settings** menu are displayed for all users, even if users are not site owners, as they may be [SharePoint Group](#) owners, in which case they have permissions to [add/remove users](#) to/from a SharePoint Group and can report on who has permissions in that SharePoint Group. The DeliverPoint links on the **Settings** menu can be restricted to site collection administrators only, see [Restricting access to DeliverPoint](#).

The two DeliverPoint links at the bottom of the **Settings** menu and on the **Site Settings** page are:

- **DeliverPoint.** Use this option to display the [DeliverPoint dashboard](#) where you can manage permissions on any site in your SharePoint deployment. By default the [farm centric](#) tree view of your SharePoint deployment is displayed.

Note. DeliverPoint is security trimmed so that those using it can only see information and perform DeliverPoint operations within their native scope of authority that is defined within SharePoint.

- [Discover Site Permissions.](#) Navigate to a site where you want to know who has permission to the site. It expands the Active Directory and SharePoint group membership in an easy to-read report so you can see who has permissions to a site. You can also generate the same reports using the farm centric tree view, which you can display by clicking **DeliverPoint** from the **Settings** menu.



If you are a SharePoint farm administrator and you use the SharePointCentral Administration web site, there is a third option on the **Settings** menu: [DeliverPoint Configuration](#) that allows you to modify [DeliverPoint configuration settings](#) at the farm level.

References

- [← Permission Management](#)
- [DeliverPoint dashboard >>](#)
- [Discover Permissions →](#)

DeliverPoint dashboard

When you click **DeliverPoint** from the [Settings](#) menu, the DeliverPoint dashboard is displayed, which allows you to complete your [permission management](#) tasks on any SharePoint object, such as, a site or a site collection, depending on the permissions you have on that object.

The screenshot shows the DeliverPoint dashboard interface. Red dashed boxes and arrows highlight the following components:

- Tree view:** A hierarchical tree on the left showing the site structure, including 'Server Farm', 'intranet.dp.local', and 'Demos'.
- Results pane:** The main area on the right displaying 'Demos Web Properties' and 'Aggregate Data'.
- Interrogation status area:** A section at the bottom left showing 'Demos Site' and 'Last Interrogation: 27 OCT at 02:41PM'.
- Properties pane:** A section at the bottom right showing site statistics: 'Sites and Workspaces:16', 'Recycle Bin:2', 'Permission Inheritance:Unique', 'Permissions Managed By:Demos', and 'Last Modified:undefined'.

The top navigation bar includes 'SharePoint', 'Newsfeed', 'OneDrive', and 'Sites'. The 'COMMANDS' tab is active, showing various tools like 'Discover Permissions', 'Permission Inheritance', 'Properties', 'Open', 'Copy Permissions', 'Grant Permissions', 'Transfer Permissions', 'Delete Permissions', 'Dead Accounts', 'Compare Permissions', 'Copy Site Permissions', 'Unique Lists', 'Copy List Permissions', and 'View Folders'.

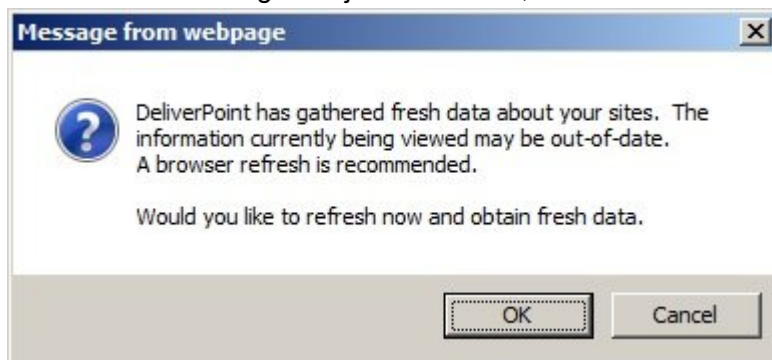
	New	Aging	Old	Empty	Small	Medium	Large
Sites (1)	0	0	1	0	0	0	1
Subsites (27)	0	1	26	0	24	1	2
Lists (243)	0	17	226	6	230	5	2



If you are using a trial version of DeliverPoint, and your trial period has expired, then when you try to display the DeliverPoint dashboard, a message is displayed in the results pane:
Trial period for product DeliverPoint 2013 has been expired. Activate
 Click **Activate** to display the [Licensing of Product 'DeliverPoint 2013'](#) page.

The dashboard page is divided into areas and commands are displayed on contextual Ribbon tabs as described below:

- **Tree view area.** When the DeliverPoint dashboard is first displayed, in the tree view area, each Web Application in your SharePoint farm is shown. This is known as the [Farm Centric](#) view. The tree view area can also be used to display an [Account Centric](#) view. You can switch between the two views using the **View** menu. Your SharePoint farm administrator can modify how the SharePoint objects are displayed in the [tree view](#).
- **Results pane.** As you complete different permission related tasks using DeliverPoint commands, the results pane is used to display the results of those tasks. Some DeliverPoint commands do not use the results pane, but open new windows. When you first display the DeliverPoint dashboard, the result pane displays information on how to use the commands on the View Ribbon tab, navigate the tree view, and a [legend](#) of the icons that appear in the tree view.
- **Interrogation status area.** This area displays the date and time that the SharePoint farm was last [crawled](#). A dialog box will from time to time be displayed, if DeliverPoint has recognised that the DeliverPoint interrogation jobs have run, and that the data on the dashboard may be out-of-date.

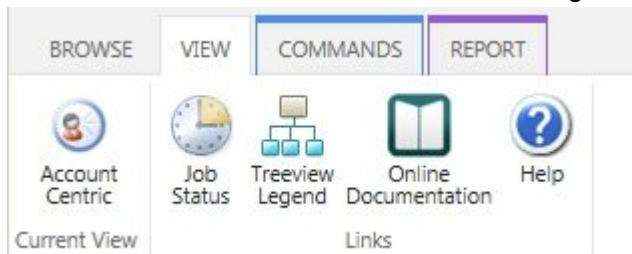


- **Properties pane:** Used to display an operation summary of the object selected. The properties pane is displayed only when using the [Farm Centric](#) view.

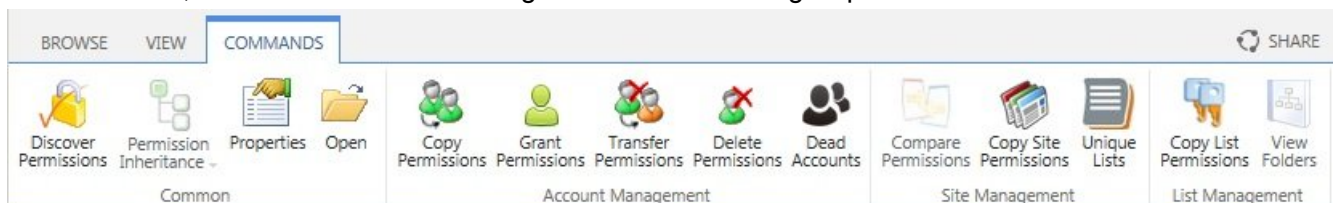
✿ **Note.** DeliverPoint dashboard is [security trimmed](#) so that those using it can only see information and perform DeliverPoint commands within their native scope of authority that is defined within your Microsoft® SharePoint® deployment.

The **DeliverPoint dashboard** consists of the following Ribbon tabs:

- **View.** This Ribbon tab contains the following commands:



- [Farm Centric](#). This command is only visible when you are in *Account Centric* view. Use to display the farm centric view in the tree view area
 - [Account Centric](#). This command is only visible when you are in *Farm Centric* view. Use to display the account centric view in the tree view area.
 - [Job Status and History](#). Use to display the Job Status and History page.
 - [Treeview Legend](#). Displays a legend of the icons used in both the farm centric and account views,
 - **Online Documentation**. Displays the online documentation for DeliverPoint 2013.
 - **Help**. Displays the LightningTools support centre where you can submit support tickets and search the support knowledge base. Anyone can submit a support ticket, however if you register with the LightningTools support centre you will be able to track the progress of any support tickets you raise.
- **Commands.** This contextual Ribbon tab is displayed when a SharePoint object is selected in the treeview area, and contains the following contextual Ribbon groups and commands:



- [Common](#), which contains the commands:
 - [Discover Permissions](#)
 - [Permission Inheritance](#) split button, with the commands Inherit Permissions and Break Permissions.
 - [Properties](#)
 - **Open**. Use this command to open the default page for the SharePoint object in a new tab in the browser. This is an easy way of quickly navigating to the SharePoint object.
- [Account Management](#)
 - [Copy Permission](#)
 - [Grant Permissions](#)
 - [Transfer Permissions](#)
 - [Delete Permissions](#)
 - [Dead Accounts](#)

- [Unique Permissions](#). This command is only available if you are using the [Account Centric](#) view.
- [Site Management](#)
 - [Compare Site Permissions](#)
 - [Copy Site Permissions](#)
 - [Unique Lists](#).
- [List Management](#)
 - [Copy List Permissions](#)
 - View Folders
- **Report**. This contextual Ribbon tab is display when DeliverPoint commands use the results pane to display the outcome of the tasks. The tabs contains one Ribbon group, which contains commands relative to the results that are displayed, for example.
 - **Export to Spreadsheet**. Use this command to export the outcomes of the DeliverPoint command to an Microsoft Excel spreadsheet.
 - Delete Accounts



Other DeliverPoint pages may contain other DeliverPoint Ribbon tabs, Ribbon groups and commands.

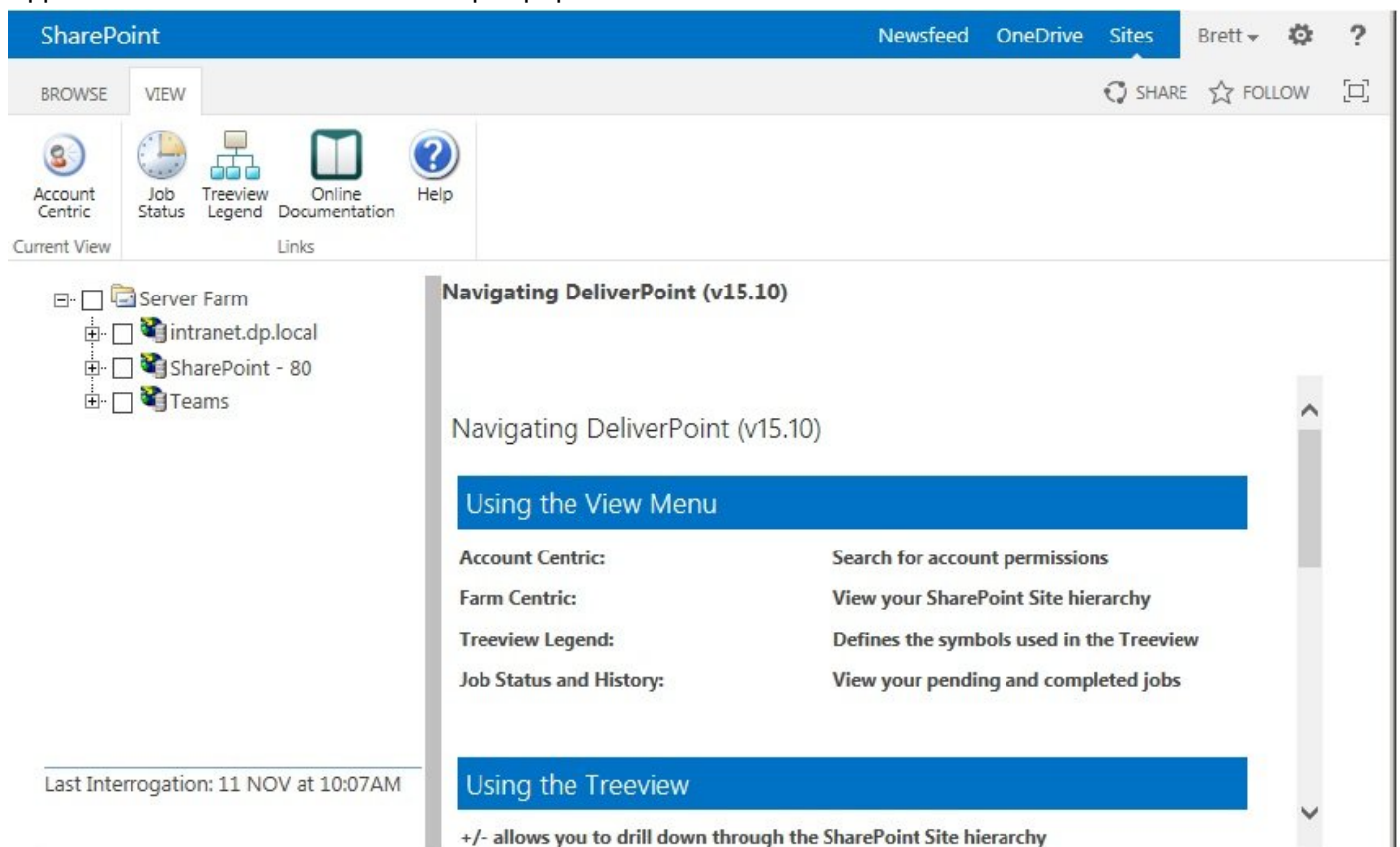
References

- [<< DeliverPoint Settings options](#)
- [Farm Centric view >>](#)
- [Account Centric View →](#)
- [Treeview Legend →](#)
- [Job Status and History page →](#)
- [Permission Management →](#)

Farm Centric view

The *Farm Centric* view is displayed by default when you first display the [DeliverPoint dashboard](#) and presents farm-wide information in an organized, efficient manner. DeliverPoint uses the concept of Incremental Data Disclosure (IDD) throughout the tree view. By clicking the plus signs (+) to the left of a SharePoint object, the user is presented with information only after they have expanded that part of the SharePoint hierarchy. This method of displaying permission across the SharePoint farm improves performance; thereby only a subset of the farm's SharePoint objects are queried and loaded into the interface at any given time.

The Farm Centric view consists of a root node called **Server Farm** . Under this node, all Web Applications  within the farm are pre-populated.



SharePoint Newsfeed OneDrive Sites Brett ?

BROWSE VIEW SHARE FOLLOW

Account Centric Job Status Treeview Legend Online Documentation Help

Current View Links

Server Farm

- intranet.dp.local
- SharePoint - 80
- Teams

Navigating DeliverPoint (v15.10)

Navigating DeliverPoint (v15.10)



Using the View Menu



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

Last Interrogation: 11 NOV at 10:07AM

When the user clicks, the plus sign (+) to the left of each Web Application, known as expanding, the managed paths  created within that Web Application are displayed. Clicking + on a managed path, all site collections  contained within the managed path are displayed. Enumeration continues in this manner, one layer per click, stopping at the individual site level, also known as the web level. Therefore when a user

expands a site collection, the top-level site of the site collection is displayed  and then expanding the top-level site, all sub sites  within that site collection are displayed.







Note that those nodes that inherit permissions from parent nodes have their icons dimmed  in the interface. Those nodes that have unique, assigned permissions have their icons actively colored  (not dimmed). This is how users can visually tell where permission inheritance is inherited or is broken in any given site collection. If a site has lists, folders, or list items with unique permissions, the web icon will have a slash  through it.

When you select a SharePoint object in the tree view, then the **Commands** Ribbon tab is displayed, which you can then use to report or complete permission related tasks.

References

- [<< DeliverPoint dashboard](#)
- [Account Centric view >>](#)
- [Tree view legend →](#)
- [Permission Management →](#)

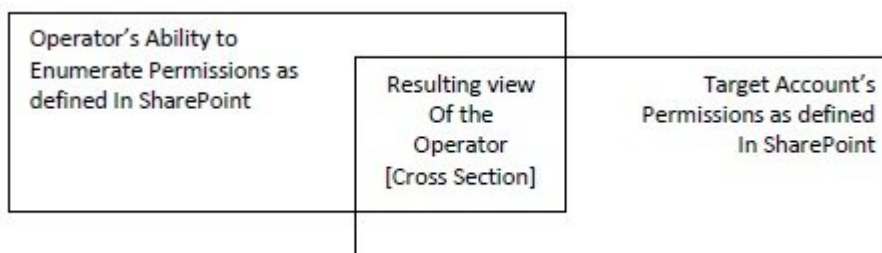
Account Centric view

The Account centric view is displayed using the [View](#) Ribbon tab on the [DeliverPoint dashboard](#). Type an account or email in the search criteria text box, and then press Enter or click the white arrow icon with a green background. You can type your user name or the name of another user. The page refreshes and the account appears in the treeview portion of the DeliverPoint dashboard. You use the same method of expanding the tree view on the *Account Centric* view as you do on the [Farm Centric](#), that is, click the plus icon (+) to the left of the account to see every web application , managed path , site collection  and sites  the account has access to. The Account Centric tree view uses the [same icons](#) as the [Farm Centric](#) tree view.

If you wish to audit another user but do not know their exact account name or email address, then you can type part of their account name, for example, **p** in to the search criteria text box. This will return all accounts with a login name or display name starting in **p**.

Only the first 50 accounts found that satisfy the search criteria are returned. If you do not find the account you are searching for, try a more specific search. When you select an account name or a SharePoint object in the tree view, then the **Commands** Ribbon tab is displayed, which you can then use to report or complete permission related tasks.












The tree view is security trimmed and only displays the intersection of the SharePoint object that you (operator) are allow to access and the SharePoint objects that can be accessed by the person (target) you selected in the tree view, as shown in the diagram below. Therefore, once you have found the target account, you may need to expand the nodes in the tree view to see where the user has access within the your permission scope.



References

- [<< Farm Centric view](#)
- [Tree view legend >>](#)

Tree view legend

Icon	Description
	Server Farm.
	Web Application.
	managed path.
	site collection.
	Site with unique permissions, that is, the site does not inherit its permissions from a parent site. The site defines its own permissions. The top-level site of a site collection is always a site with unique permissions.
	Site that inherits permissions from parent site. When you create a sub site, the default is always to inherit its permissions from the parent site.
	The site contain broken inheritance at the list, library or folder level.
	Site no access. The current user does not have access to this site.
	Unknown access. The current user does not have access to view another user's permissions on this site.
	Account
	Segment. In a SharePoint farm when a Web Application contains more than 100 site collections or sites the tree view is segmented for easier navigation. The Display Segment value can be changed by your SharePoint farm administrator. The default value is 100.

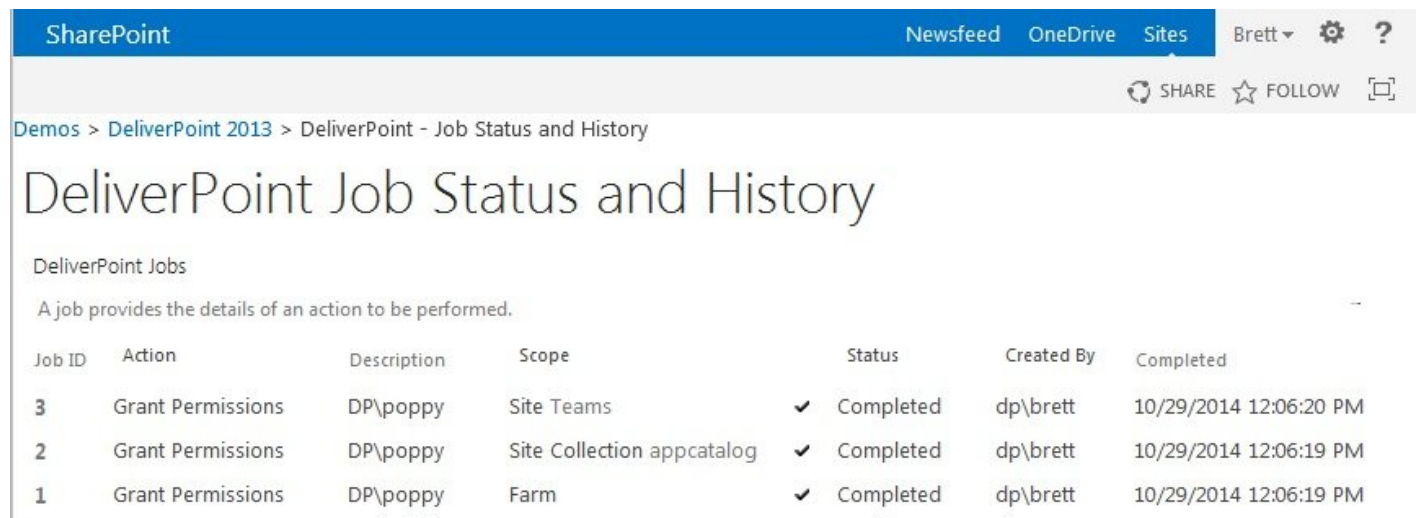
References

- [Farm Centric View →](#)
- [Account Centric View →](#)

Job Status and History

A DeliverPoint action results in the creation of a DeliverPoint job. DeliverPoint jobs are queued and processed by the [DeliverPoint Job Execution](#) SharePoint timer job, which runs by default every 5 minutes. The **DeliverPoint Job Status and History** page provides a summary of DeliverPoint jobs and is displayed when:

- **Job Status** command is clicked from the [View](#) Ribbon tab on the [DeliverPoint dashboard](#),
- **Job Status** is clicked on the *Operation* screen in the results pane, that appears when you have completed configuring a DeliverPoint action and confirmed that you have correctly configured the action.



Job ID	Action	Description	Scope	Status	Created By	Completed
3	Grant Permissions	DP\poppy	Site Teams	✓ Completed	dp\brett	10/29/2014 12:06:20 PM
2	Grant Permissions	DP\poppy	Site Collection appcatalog	✓ Completed	dp\brett	10/29/2014 12:06:19 PM
1	Grant Permissions	DP\poppy	Farm	✓ Completed	dp\brett	10/29/2014 12:06:19 PM

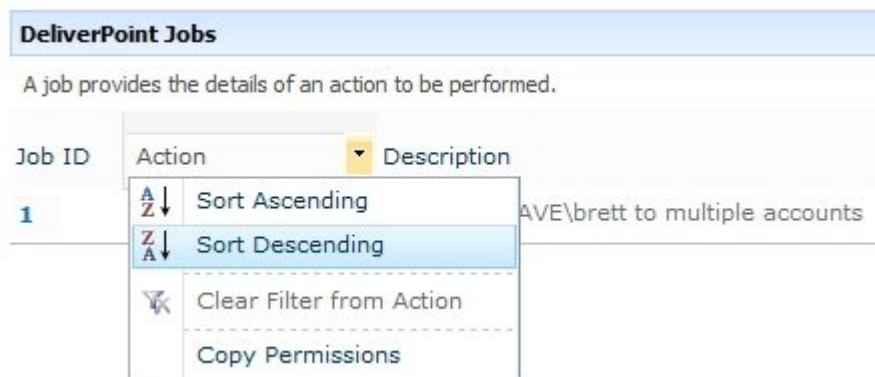
The *Job Status and History* page contains the following information:

- **Job ID.** This column displays the job number and provides a drop down menu, where you can select:
 - **View Job** to display the [DeliverPoint Job Details](#) page
 - **Initiate Rollback.** A job can only be rolled back if is carried out by mistake. You can rollback a job once the job has completed. You can also rollback a job using the [Job Details](#) page.
 - **Cancel.** A job can only be cancelled if is in Pending state. You can also cancel a job using the [Job Details](#) page if the job is still pending.

LightningTools DeliverPoint Jobs



- **Action.** This column displays the DeliverPoint action, such as [Copy Permissions](#). The column heading can be used to sort or filter the DeliverPoint jobs on the page.



- **Description.** This column displays a summary of the DeliverPoint action to be completed, for example, *'LightningTools\brett to LightningTools\steve'*.
- **Scope.** This column displays the SharePoint objects that were affected by DeliverPoint action, for example, *Site LT*, where *Site* identify that the scope was a site, and *LT* is a hyperlink to the site collection selected.
- **Status:** This column details the status of the job, and can be one of the following values. The column heading can be used to sort or filter the DeliverPoint jobs on the page.
 - **Pending.**
 - **Processing.**
 - **Warning.**

- **Cancelled.**
- **Rollback Completed.**
- **Completed.** When a job is successfully completed a tick icon is displayed to the left of *Completed*.

Note Pending jobs are displayed at the top of the list.

- **Created By.** This column details the user name who initiated the DeliverPoint action. The column heading can be used to sort or filter the DeliverPoint jobs on the page.
- **Completed.** This column details the date and time the DeliverPoint action was completed. The column heading can be used to sort or filter the DeliverPoint jobs on the page.

Jobs classified as [Run Now](#) will be processed the next time the [Job Execution](#) SharePoint timer job runs, which by default is every 5 mins. Jobs classified as [Run Later](#) will be processed the next time the SharePoint Interrogation timer job runs. If a job was created with a transaction type of [Both](#), two separate but identical jobs, a [Run Now](#) job and a [Run Later](#) job, will be created.

On the **DeliverPoint Job Status and History** page, selecting a specific job will display the details of the job. Within the details, information, details, statistics, and tasks are displayed.

References

- [← DeliverPoint dashboard](#)
- [Job Details page >>](#)

Job Details page

A DeliverPoint action results in the creation of a DeliverPoint job. DeliverPoint jobs are queued and processed by the [DeliverPoint Job Execution](#) SharePoint timer job, which runs by default every 5 minutes. The **Job Details** page displays information for a DeliverPoint job and contains four sections as detailed below:

Demo

🔍

DeliverPoint Job Details

[DeliverPoint Jobs](#)

Job Information

Job ID:	2
Action:	Copy Permissions
Description:	DP\phill to DP\charlotte
Scope:	Site Demo
Created By:	SHAREPOINT\system

Job Details

Transaction Type:	Run Now
Details Summary:	Copy permissions of DP\phill to DP\charlotte in Site

Job Statistics

Status:	Completed (Rollback)
Submitted:	6/20/2016 12:09:15 PM
Started:	6/20/2016 12:10:48 PM
Completed:	6/20/2016 12:10:49 PM
Job Duration (seconds):	1.803

▲ [Job Actions](#)

Action	Status
Starting Job 2	Info

- **Job Information.** This section contains:
 - **Job ID.** A unique number assigned to the DeliverPoint action.
 - **Action.** The DeliverPoint action to be completed, for example, [Transfer Permissions](#).
 - **Description.** This displays the DeliverPoint action to be completed, for example, *'LightningTools\brett to LightningTools\steve'*.

- **Scope.** Displays the SharePoint objects that were affected by DeliverPoint action, for example, *Site LT*, where *Site* identifies that the scope was a site, and *LT* is a hyperlink to the site collection selected.
- **Created By.** Details the user name who initiated the DeliverPoint action.
- **Job Details.** This section details:
 - [Transaction Type](#).
 - **Include Alerts.** The value will be **on** or **off**, depending on your choice when you configured the DeliverPoint action.
 - **Details Summary.** This contains a summary of the action to be completed, for example, *'Transfer TRAINSBYDAVE\brett to TRAINSBYDAVE\steve in Site http://intranet/divisions/LT'*.
- **Job Statistics.** This section contains:
 - **Status.** This indicates the status of the job:
 - **Pending.** When a job is in this state then, you will be provided with a link to **Cancel** the job.
 - **Processing.**
 - **Warning.**
 - **Cancelled.**
 - **Completed**
 - **Rollback Completed**
 - **Submitted.** The date and time the DeliverPoint job was submitted.
 - **Completed.** The date and time the DeliverPoint job was completed.
 - **Job Duration (seconds).** The duration in seconds that it took the DeliverPoint job to be processed.
- **Job Tasks.** This section contains a list of all tasks that a DeliverPoint job needed to complete.

References

[<< Job Status and History](#)

[Transaction Types >>](#)

Transaction Types

A DeliverPoint action results in the creation of a DeliverPoint job. DeliverPoint jobs are queued and processed by the [DeliverPoint Job Execution](#) SharePoint timer job, which runs by default every 5 minutes. When a user configures a DeliverPoint action, they specify a **Transaction Type** which identifies when a DeliverPoint action should be processed. There are three Transaction Types for job processing:

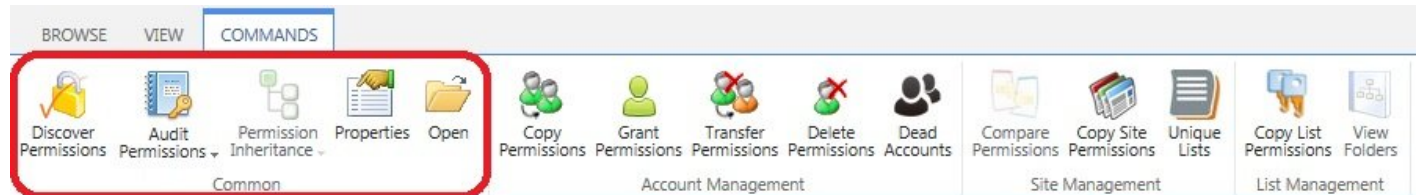
- **Run Now:** Transactions are queued for immediate processing and will use the current information in the DeliverPoint database to make the requested changes to your farm. Transactions will only be guaranteed to be as complete as the start date and time of the last successful interrogation.
- **Run Later:** Transactions are queued for processing after the next interrogation. This transaction will be guaranteed complete at the date and time the interrogation finished.
- **Both:** Both **Run Now** and **Run Later** jobs are created. The advantage to running the same job twice is to accommodate for the chance a production environment is different or more up-to-date than the environment known to the DeliverPoint databases. Since the individual job executions are built using the information in the DeliverPoint database, there is always the possibility that the DeliverPoint database is not 100% in synch with your production farm. The updates in the production environment are picked up at the next interrogation, so running an identical job again to ensure your operation used the most up-to-date production information.

References

- [← Job Status and History](#)
- [<< Job Details page](#)
- [Common Commands >>](#)
- [Site Management →](#)

Common Commands

There are a number of DeliverPoint commands that can be used, whether you are managing permissions for an account, farm, managed path, site collection, sites, lists, libraries or items. These commands can be found in the Common group on the Commands Ribbon tab.



- [Discover Permission](#)
- [Audit Permissions](#)
- [Permission Inheritance](#)
- [Properties](#)
- **Open** the SharePoint object in a new browser windows / tab.

[<< Transaction Types](#)

[Discover Permissions >>](#)

Discover Permissions

‘Discover who has permissions to this SharePoint object’

Discover Permissions allows the user to find out who has access to a given object and how that access is given.

✿ **Note:** Discover Permissions is mostly a real-time feature. If an account is assigned a new permission level to an object, the account will be found immediately in the [Discover Permissions report](#) for the object. The only exception is when an Active Directory group which has not been crawled by the [Authentication Store Interrogation](#) is added to an object. The membership for the group will not be known until the group has been crawled.

You can only use the Discover Permission DeliverPoint action if you have the SPBasePermission Enumerate permission, that is, only users who have access to view permissions in SharePoint can access this DeliverPoint action. For example, users who are mapped to a permission level that includes the Manage Permissions right, such as, Full Control, will be able to use this action.


There are three forms of the *Discover Permissions* DeliverPoint action:

- [Discover Site Permissions](#)
- [Discover List Permissions](#)
- [Discover Item Permissions](#)

All three forms of this DeliverPoint action uses the [Discover Permissions with DeliverPoint 2013 page](#) results page, which you can use [to filter the results](#). The [Discover Permissions with DeliverPoint 2013 page](#) and [how to filter the results](#) are explained in the next sections. You can also add a column a list / library, based on the [DeliverPoint inheritance field](#) to display folder, list item, file permission inheritance in views.

Discover Site Permissions

To use the **Discover Site Permissions** action, either:

1. In the browser, navigate to the SharePoint site where you want to complete the action, click **Settings**  , and click **Discover Site Permissions 2013** to open a new browser window displaying the [Discover Permissions with DeliverPoint 2013](#) page.

or complete the following steps:

1. Navigate to the [DeliverPoint dashboard](#) and using the **View** Ribbon tab, click either [Farm Centric](#) or [Account Centric](#).
2. In the tree view, select those nodes, also known as SharePoint objects, to be included in the scope, for example, one or more site collections or sites. The *Discover Permissions* command cannot be completed on an accounts. In the properties of the node selected are displayed in the dashboard's **Properties** pane.

Note: Child nodes are not automatically included.

3. On the **Commands** Ribbon tab, click **Discover Permissions** in the [Common](#) group.



Note When you have a small screen resolution the commands in the **Common** group are available from the **Common** split button.

A new browser window opens and displays the [Discover Permissions with DeliverPoint 2013](#) page.

[← Go to top of section](#)

Discover List Permissions

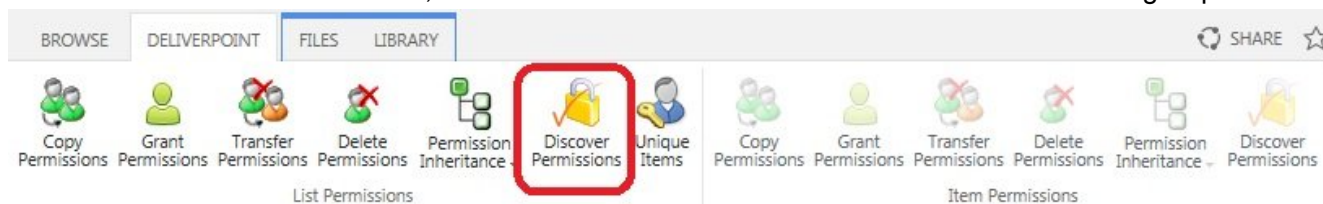
To use the **Discover Lists Permissions** action, complete either:

1. If [lists and libraries are displayed in the tree view](#) on the [DeliverPoint dashboard](#), select one or more lists or libraries to be included in the scope.
2. On the **Commands** Ribbon tab, click **Discover Permissions** in the [Common](#) group.

or complete the following steps:

1. Navigate to the list where you want to discover permissions.

- On the **DeliverPoint** Ribbon tab, click **Discover Permissions** in the **List Permissions** group.



Note When you have a small screen resolution the commands in the **List Permissions** group are available from the **List Permissions** split button.

The [Discover Permissions with DeliverPoint 2013 page](#) is displayed.

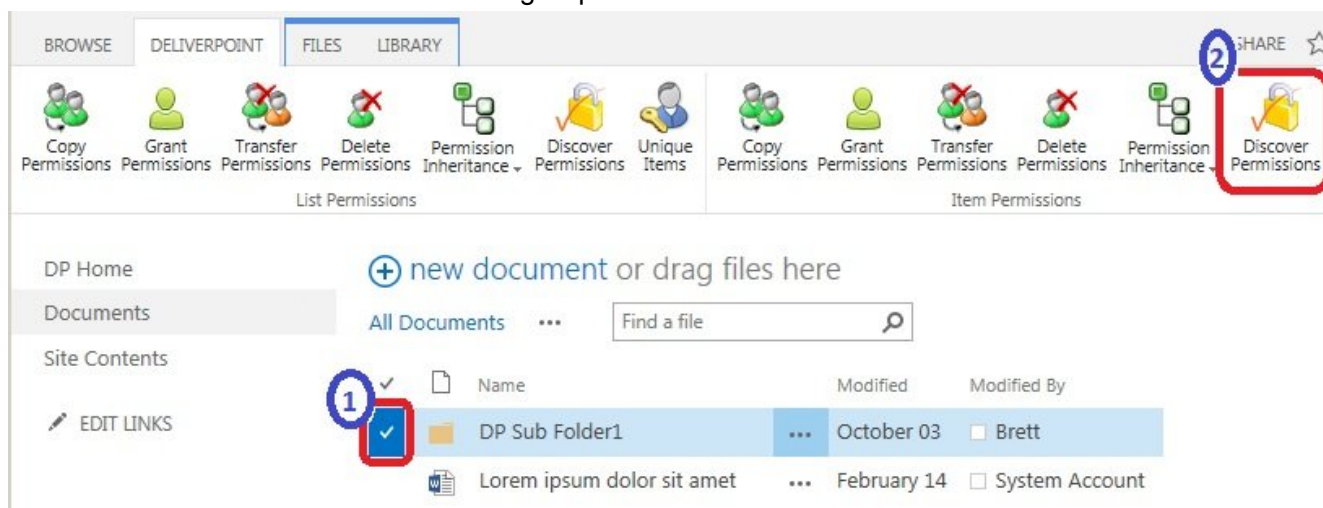
Tip: Information on the *Unique Items* command on the *DeliverPoint* Ribbon tab, can be found in the [Unique List Items Detection](#) section later in this documentation.

[← Go to top of section](#)

Discover folder or item Permissions

To use the **Discover Permissions** action on a folder, list item or file, complete the following steps:

- Navigate to the list where you want to use the DeliverPoint *Discover Permissions* command.
- Click to the left of the folder, list item or file, and then on the **DeliverPoint** Ribbon tab, click **Discover Permissions** in the **Item Permissions** group.



The [Discover Permissions with DeliverPoint 2013 page](#) is displayed.

References

[← Go to top of section](#)

[<< Common Commands](#)

[Discover Permissions results page >>](#)

Discover Permissions results page

The [Discover Permissions](#) results are batched as 100 results per page. At the bottom of the page there are page numbers you use to display each set of 100 results. You can also [schedule the reports to be generated](#) every min, hour, daily, week and monthly.

SharePoint

NewsfeedOneDriveSites

Brett

BROWSECOMMANDS

SHAREFOLLOW

Copy Permissions

Grant Permissions

Transfer Permissions

Delete Permissions

Permission Inheritance

Permission Management

Export to Spreadsheet

Schedule

Reporting

View Scope

Show Administrators

Nested Groups

Direct Groups

Display Options

Online Documentation

Help

Links

Home

Site

User Name

Permissions

Permissioned Via...

Lists

☐ Demos administrator Full Control (Implicit) Site Collection Administrators

Documents

☐ Demos Brett Full Control (Implicit) Site Collection Administrators

Access Apps

Asset Tracking

☐ Demos Brett Full Control (Implicit) Site Collection Administrators

Issue Tracking

☐ Demos Sara Full Control (Implicit) Site Collection Administrators

Orders and Products

☐ Demos SP Admin Full Control (Implicit) Site Collection Administrators

Subsites

Data Viewer

☐ Demos administrator Full Control Teams Owners

DeliverPoint

☐ Demos Brett Full Control Teams Owners

The page contains the following columns:


- **Site / List / Item.** When the hyperlink is clicked the home (default) page of the site / list or the property page of the list item / file is displayed.
- **User Name.** The account's Display Name.
- **Permissions.** the permission level(s) that is mapped to the account on the object. Multiple permission levels are not listed separately.
- **Permissioned Via.** Lists graphically how the user has been given access to the object. To expand SharePoint Groups, click the plus sign (+) to the left of the group name.

✳ When the **Show Lists and Libraries In Report** and / or **Show List and Library Items In Report** check boxes are selected on the [DeliverPoint Configuration](#) page, then this report can also contain list, library, list item and file permission information.

Sorting the results

You can sort the results using the column headings **Site**, **User Name**, **Permissions** and **Permission Via**. Sorting is completed against all the results returned, that is, sorting is not limited to the 100 results displayed on a specific page when there are more than 100 results are returned.

Filtering the results

The commands in the [Display Options](#) Ribbon group, and the [Filter](#) icon  displayed to the right of each column heading can be used to refine the results returned. See the [next section](#) for more information on how to filter the results of the discover permission action.

Exporting the results

To export the results, click **Export to Spreadsheet** on the **Commands** Ribbon tab, in the **Reporting** group. The Microsoft® Excel spreadsheet file name is of the format, *Discover_Permissions_yyyymmdd.xls*. All results are exported, that is, the result exported are not limited to the results displayed on a specific page when more than 100 results returned from the *Discover Permissions* command.

Scheduled Reporting

To schedule a permissions report, click **Schedule** on the **Commands** Ribbon tab, in the **Reporting** group to display the **Schedule Discover Permissions Report** dialog.

Schedule Discover Permissions Report

X

Folder Path	Folder Path
Specify path of the folder where report must be created	<input type="text" value="http://intranet.dp.local/sites/LT/Shared%20Documents/"/>
File Name Pattern	File Name Pattern
Specify pattern used for generating file name of the report	<input type="text" value="Discover_Permissions_[MM].[dd].[yyyy]_[HH].[mm].[ss]_[USER]"/>
Schedule	The report is scheduled to be generated at
Specify schedule of report generation	<input checked="" type="radio"/> Minutes Every <input type="text" value="15"/> minute(s)
	<input type="radio"/> Hourly
	<input type="radio"/> Daily
	<input type="radio"/> Weekly
	<input type="radio"/> Monthly
Options	<input type="checkbox"/> Generate Once
Specify additional options	
Last Run	11/13/2014 5:15:45 PM
Shows when last time the report has been generated	
	<div><div>Save</div><div>Clear</div><div>Cancel</div></div>

1. In the **Folder Path** text box, type the document library where you want to store the report.
2. In the **File Name Pattern** text box, type the pattern to be used to generate the file name of the report.
By default the pattern is, **Discover_Permissions_[MM].[dd].[yyyy]_[HH].[mm].[ss]_[USER]**
3. In the **Schedule** section specify when the report should be generated. You can select one of the following schedules:

- **Minutes** Every 1 to 59 minutes.
 - **Hourly**
 - **Daily**
 - **Weekly**
 - **Monthly**
6. In the **Options** section, select the **Generate Once** check box, if you want the report to be generated once.
 7. Click **Save**.

To modify the schedule, click **Schedule** on the **Commands** Ribbon tab. The **Schedule Discover Permissions Report** dialog will display the last time the report was generated. The *Last Run* on the *Schedule Discover Permissions Report* dialog is only displayed when you are modifying an existing schedule.

To remove the schedule, click **Schedule** on the **Commands** Ribbon tab, and then at the bottom of the **Schedule Discover Permissions Report** dialog, click **Clear**.



The scheduled Discover Permissions reports are generated by the [DeliverPoint Job Execution SharePoint timer job](#), and therefore the generated *Discover Permissions* reports are not created more frequently than the execution of the [DeliverPoint Job Execution timer job](#). For example, by default the [DeliverPoint Job Execution timer job](#), executes every 5 minutes, therefore, although a *Discover Permissions* report can be scheduled to be generated every minute, they will only be generated every 5 minutes.

The schedules for *Discover Permission* reports are registered in the *ReportSchedules* table in the [DeliverPoint database](#). Database administrators can find all scheduled reports by querying that database table.

References

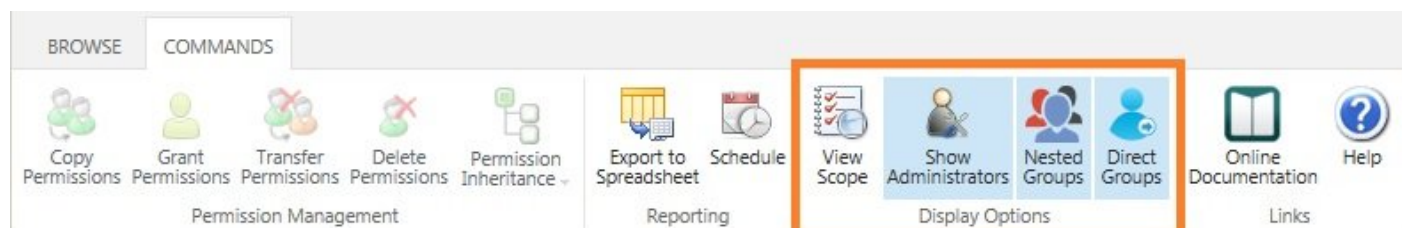
[<< Discover Permissions](#)

[Refining Discover Permissions results >>](#)

Refining Discover Permissions results

The [Discover Permission](#) results can be customized, using either the commands in the [Display Options](#) group on the **Commands** Ribbon tab, or using the [Filter](#) icon  to the right of the column headings.

Display Options



- **View Scope.** Select this command if you wish to display the SharePoint objects selected, for example, when you have selected multiple folders and / or items and then clicked the *Discover Permissions* in the *Item Permissions* group on the *DeliverPoint* Ribbon tab, the **Scope** section would display all the folders / items you selected. The *managed by* SharePoint object refers to the object from which the selected object is receiving its permission configuration from. For example, in the following diagram, the *docx* file is inheriting it's permissions from the Demos site as is the folder *DP Folder 2*. This indicates that permission inheritance has not been broken from the default settings; whereas the permission inheritance for the folder *DP Folder 1* is itself which indicates permission inheritance was broken at this folder level. By default, the *Scope* section is not displayed.

▲ Scope

Items

SPS2014_Speaker_Submission.docx managed by Demos

DP Folder 1 managed by DP Folder 1

DP Folder 2 managed by Demos

- **Show Administrators.** Use to include or exclude site collection administrators in the results ONLY if you are a site collection administrator. This option is grayed out if you are not site collection administrators. The *Show Administrators* command is a toggle switch. By default, the *Show Administrators* command has a blue background which is used to show that users who are members of the *Site Collection Administrators* group are displayed in the results. When the *Show Administrators* command is not selected, that is, it has a white background, the *Site Collection Administrators* group will not be displayed in the *Permissioned Via* column.
- **Nested Groups.** Use to include or exclude users who have been given permission directly through nested Active Directory (AD) groups. For example, when *Brett* is a member of the *g_Sales* AD group,

which is nested inside the *g_Employees* AD group, and the *g_Employees* AD group is mapped to the *Edit* permission level on a SharePoint object, such as, a site, then when the *Nested Groups* command is selected, that is, when it has a blue background, then *Brett* is displayed in the results. By default users who gain access to a SharePoint object because they are in a nested AD group are displayed in the results.

- **Direct Groups.** Use to include or exclude users who have been given permission directly using Active Directory (AD) groups. For example, when *Brett* is a member of the *g_Sales* AD group, and the *g_Sales* AD group is mapped to the *Edit* permission level on a SharePoint object, such as, a site, then when the *Direct Groups* command is selected, that is, when it has a blue background, then *Brett* is displayed in the results. Users who only gain access through nested AD groups on a SharePoint object will not be displayed when the *Direct Groups* command is selected. By default, users who gain access to a SharePoint object because they are included in an AD group that is mapped directly to a permission level on a SharePoint object are displayed in the results.

The labels in the following diagram shows the affect of selecting the commands in the **Display Options** group on the **Commands** Ribbon tab.

1. The **Scope** section is displayed when the **View Scope** command is selected.

Site	User Name	Permissions	Permissioned Via...
<input type="checkbox"/> Demos	Brett	Full Control (Implicit)	Site Collection Administrators Brett
<input type="checkbox"/> Demos	Brett	Full Control (Implicit)	Site Collection Administrators
<input type="checkbox"/> Demos	Brett	Full Control	Teams Owners Brett
<input type="checkbox"/> Demos	Brett	Read	Teams Visitors DP\domain users Brett
<input type="checkbox"/> Demos	Brett	Edit	Teams Members DP\g_itsupport g_spadmins Brett




Users added directly to SharePoint Groups are always displayed



1. The **Scope** section is displayed when the **View Scope** command is selected.

2. Users in the *Site Collection Administrators* group are displayed when the **Show Administrators** command is selected.
3. Users in *Active Directory* groups are displayed when the **Direct Groups** command is selected.
4. Users in *nested Active Directory* groups are displayed when the **Nested Groups** command is selected.

✿ By default, when the discover permissions page is displayed the Ribbon commands, **Show Administrators**, **Nested Groups** and **Direct Groups** are selected. If you only want to display users who have access to SharePoint objects when they are directly added to a SharePoint group, then clear both the **Nested Groups** and **Direct Groups** commands.


Column Heading Filtering

Use the *Filter* icon  displayed to the right of each column heading to filter the *Discover Permissions* results by *Site*, *User Name*, *Permissions* or *Permissions Via*. When a filter is configured for a column heading then the *Remove Filter* icon  is displayed to the right of the *Filter* icon .


When you click the *Filter* icon  a dialog box opens that allows you to configure one or more filter criteria. By default the *Filter By* dialog contains three drop down lists for you to configure one filter criteria, to add another criteria, select either **And** / **Or** and then click the green plus icon  :

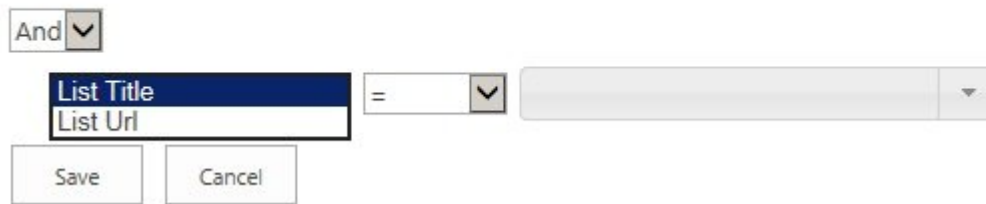
- Click **And** to create a filter where the data must match the criteria in all filter criteria.
- Click **Or** to create a filter where the data must match the criteria in only one filter criteria.

Each criteria can be removed from the filter by clicking the remove filter icon .




Once the filter is configured click **Save**. To edit an existing filter, click the *Filter* icon  again.

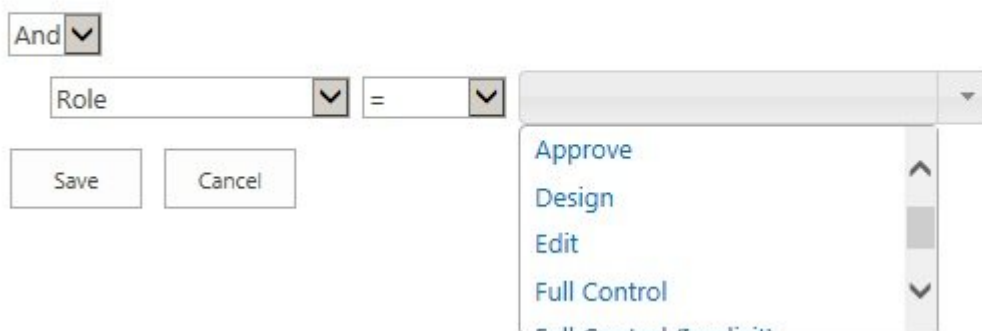
Each filter criteria consists of three input boxes:

1. Specify the format of the value in the column you wish to use, for example.
 - When you click the *Filter* icon  to the right of **Site / List / Item** column heading, the **Filter By Site**, **Filter By List** or **Filter By Item** dialog box opens, which allows you to filter the *Discover Permissions* results using either the **Site Title** or **Site Url / List Title** or **List Url / Item Title** or

Item Url.**Filter By List**


The dialog box titled "Filter By List" has a close button (X) in the top right corner. It contains a logical operator dropdown set to "And". Below it is a list box with "List Title" selected. To the right of the list box is an equals sign (=) followed by a dropdown arrow. Further right is a text input field for the filter value. On the far right are three buttons: a green plus (+), a blue plus (+), and a red minus (-). At the bottom are "Save" and "Cancel" buttons.

- When you click the *Filter* icon  to the right of **User Name**, the **Filter by User** dialog allows you to specify the filter criteria using the **Display Name**, **Email** or **Name**;
 - When you click the *Filter* icon  to the right of **Permissions**, the **Filter by Permission Levels** dialog allows you to filter using permission levels, whether they are the out-of-the-box permission levels or custom permission levels.
 - When you click the *Filter* icon  to the right of **Permissions Via**, the **Filter by Permission Via** dialog allows you to filter by user, Active Directory group or SharePoint Group using the **Display Name**, **Email** or **Name** fields.
5. Click the *Operation* box, and then select the operator that you want. The operations available are: **=**, **Like** or **Not Like**
 6. Click the *Value* box, and then select or type the criteria that you want, for example, when you select the *Permissions* column heading filter, the values listed in the *Value* box, will be the permissions levels displayed in the results page. When you select the *Permissions Via* column heading filter, the values lists in the *Value* box, are the users, Active Directory groups and SharePoint groups that are displayed on the results page.

Filter By Roles


The dialog box titled "Filter By Roles" has a close button (X) in the top right corner. It contains a logical operator dropdown set to "And". Below it is a list box with "Role" selected. To the right of the list box is an equals sign (=) followed by a dropdown arrow. Further right is a text input field for the filter value. On the far right are three buttons: a green plus (+), a blue plus (+), and a red minus (-). At the bottom are "Save" and "Cancel" buttons. A dropdown menu is open from the value field, showing a list of roles: "Approve", "Design", "Edit", "Full Control", and "Full Control (Anonymous)".

You can also type a value into the *Value* box, for example, you can create a filter criteria to display all

users whose name contains “an”.

Filter By User

And ▼

Name ▼ Like ▼ an ▼

Save

Cancel



References

[<< Discover Permissions results page](#)

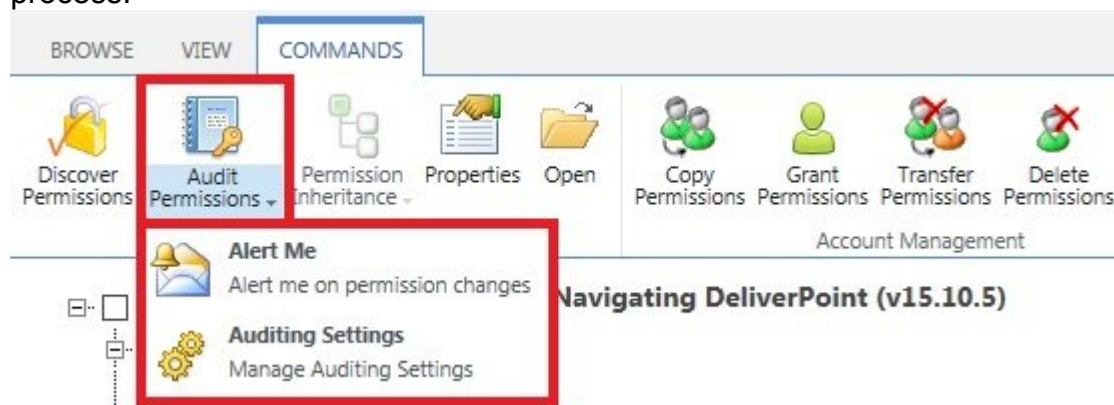
[Tracking Permission Changes >>](#)

Tracking Permission Changes

DeliverPoint provides two methods of tracking permission changes:

- [Alerts](#). Similar to [Alerts in SharePoint](#), the **Alert Me** option in DeliverPoint allows a user to track permission changes by email messages. From an infrastructure perspective, no special configuration is required for DeliverPoint Alert Me to send email messages. If users receive SharePoint Alert Me email notifications, then DeliverPoint Alert Me notifications should also work.
- [Permission Auditing reports](#).

To receive alerts or audit permission changes, you must first configure alert me or auditing in the [DeliverPoint dashboard](#) tree view and then use the **Audit Permissions** split button in the [Common](#) group on the **Commands** Ribbon. Subsequent pages in this documentation fully explain this process.



The permission changes that can be tracked are:

1. Associating or deassociating permission levels to users, Active Directory security groups and [SharePoint groups](#).
2. Breaking or the restoration of [permission inheritance](#).
3. Changes to SharePoint groups by adding or removing users or Active Directory security groups.
4. Deleting users or Active Directory security groups from a site collection.

These changes can be achieved using DeliverPoint, the out-of-the-box SharePoint 2013 web pages, Windows PowerShell or programmatically using the SharePoint APIs. Changes to permission levels are not tracked, for example, the creation of permission levels; the addition or removal of permissions to a permission level and the [management of permissions for a Web Application](#).

Note: The Alert Me and Audit functionality was first added to [DeliverPoint version](#) 15.10.5.

[<< Refining Discover Permissions results](#)

[Alerts >>](#)


Alerts

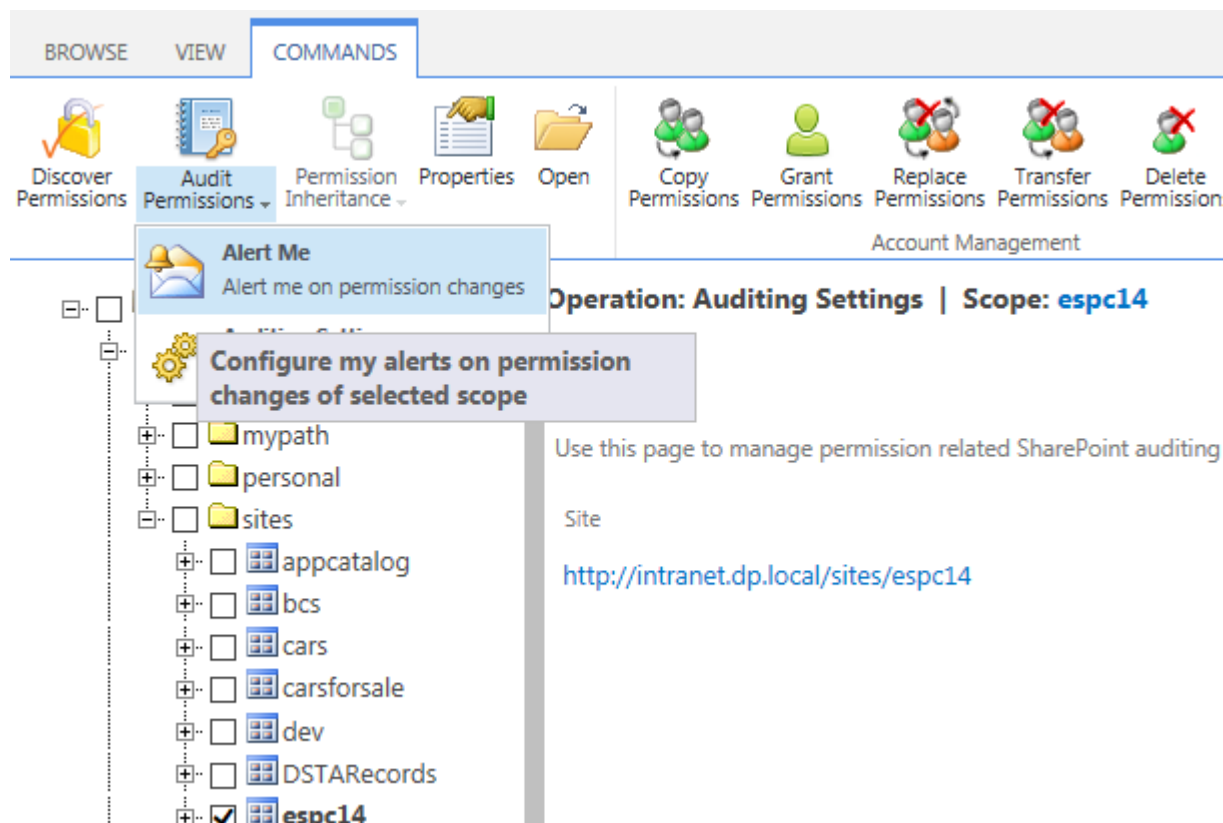
Alerts are notifications of permission changes that you receive as e-mail messages.

You can [create](#), [review](#), [modify](#) and [delete](#) alerts.

Create an alert

To configure (enable) **Alert Me**, complete the following steps:

1. Click **Settings**  and then click **DeliverPoint 2013** to display the [DeliverPoint dashboard](#), ensure the [Farm Centric view](#) is selected.
2. In the tree view, select the check box to the left of the relevant SharePoint object you wish to track. If you select more than one SharePoint object then an alert is created for each SharePoint object selected.
3. On the **Commands** Ribbon tab, click the **Audit Permissions** split button down arrow and then click **Alert Me**.



The **Operation: Alerts Management** page is displayed in the results pane of the DeliverPoint dashboard. Existing Alerts are listed on this page, which you can [modify](#) or [delete](#).

4. Click **New Alert**.

The *Create New Alert* dialog is displayed.

Create New Alert

Title

Specify title of alert.

Permission Change

Send Alerts To

Specify to whom alerts must be sent.

System Account

Change Type

Specify the type of change that you want to be alerted to.

☒ Permission Changes
 ☐ Permission Inheritance Changes
 ☐ Groups Members Changes
 ☐ Delete Users/Groups Changes

Change Initiator Pattern

Specify pattern, that will be used for filtering changes (by their initiator) for which you want to be alerted to.

Send Alerts For Changes via Parents

Specify whether you want to be alerted also for changes done in parent scopes (affecting also current scope permissions) or only for changes done in current scope directly.

☒

Role Added/Removed

Specify whether you want to be alerted for role added changes, role removed changes or for both changes.

Both

Role Name Pattern

Specify pattern, that will be used for filtering changes (by added/removed role name) for which you want to be alerted to.

5. Complete information in the following sections and then click **Create** at the bottom of the dialog. You may need to scroll down to see all the sections.

- **Title.** Type a title for the alert. This is used as the email subject.
- **Sent Alerts To.** Type the user names or email addresses of people you to be notified of permission changes. By default, the person who is creating the alert is automatically added to this text box.
- **Change Type.** Select the type of permission change you wish to track:
 - **Permission Changes.** Track permission changes are made to users, Active Directory security groups or SharePoint Groups on the select SharePoint scope, that is, send an

email message when users, Active Directory security groups or SharePoint Groups are assigned to different permission levels.

- **Permission Inheritance Changes.** Track when [permission inheritance](#) is broken or restored on the selected SharePoint scope.
- **Groups Members Changes.** Track permission changes to SharePoint groups.
- **Delete Users/Groups Changes.** Track when users or Active Directory security groups are deleted from a site collection.

Note: Once an alert has been created for a specific Change type, the alert can not be modified to a different change type. If you do select the wrong change type, you have to delete the original alert and create a new alert with the correct change type. If you want to track all change types for a specific SharePoint scope, you have to create four alerts.

- **Change Initiator Pattern.** Use this box to track permission changes by the person who makes the change. In the text box, use one of the following formats to identify the initiator's login name. You can not use their email address or display name.
 - Type the exact value of the initiator's login name, for example, **dp\penny**, where **dp** is the domain name, and **penny** is the userid.
 - Use the wildcard characters (%) or (*) to identify one or more login names, where the wildcard character represents one or more character in the login name, for example:
 - **dp\p***, or **dp\p%** to find any login name beginning with **p**.
 - **dp*ny** or **dp\%nnny** to identify any login name ending in **ny**.
 - **dp*nn*** or **dp\%nn%** to identify any login name that contains the characters **nn** in the middle of the login name.
 - Use regular expression, in the form, **R[RegEx]**, where *RegEx* is the [regular expression](#).
- **Send Alerts For Changes via Parent.** This option is only valid for the first two change types, that is, *Permission Changes* and *Permission Inheritance Changes*, and is not meaningful, for alert scopes at site collection, managed path, web application or farm. When the check box is deselected, then alerts will be sent when break or restore permission level changes occur on the selected SharePoint scope. When the check box is selected, then alerts are sent when a change occurs to a SharePoint object in the parent inheritance chain.
- **Role Added/Removed.** Select whether to track when permission levels are **Added** or **Deleted** or **Both** (default).
- **Role Name Pattern.** You can limit the notifications received by including only changes for one or more permission levels. In the text box, type:
 - The exact name of a permission level, such as, **Edit** or **Full Control**.
 - Use the wildcard characters (%) or (*) to identify one or more permission levels.
 - Use or use a [regular expression](#) to identify more than one permission level, such as, **R[Edit|Contribute]**.

When the text box is empty, permission changes that involve all permission levels are included in the notifications.


- **Member Type.** Track permission changes occur when they affect:
 - **User s** and Active Directory security groups.
 - SharePoint **Groups**.
 - **Both** (default).
- **Member Name Pattern.** You can limit the notification by filtering the permission changes to one or more users or Active Directory security groups or SharePoint groups. In the text box, type:
 - The exact name of a user or security group or SharePoint Group.
 - Use the wildcard characters (%) or *) to identify one or more users / security groups or SharePoint groups.
 - Use [regular expressions](#) to identify more than one user and / or security groups and / or SharePoint groups, in the format **R[RegEx]**.
- **When To Send.** Select how frequently you want to receive notifications:
 - **Send notification immediately.**
 - **Send a daily summary.**
 - **Send a weekly summary.** You can choose when to send the weekly notification, by default it is set to Sunday at 12 a.m.

11. At the bottom of the dialog click **Create**.



The **Operation: Alerts Management** page is display in the results pane of the DeliverPoint dashboard, summarizing the alert(s) you have created.

Modifying alerts

To modify an alert, complete the following steps:




1. Click **Settings**  and then click **DeliverPoint 2013** to display the [DeliverPoint dashboard](#), ensure the [Farm Centric view](#) is selected.
2. In the tree view, select the checkbox to the left of the SharePoint object where the alert was created. If you select more than one SharePoint object then alerts for all those objects are displayed. If you are unsure where alerts have been created, click **Server Farm**, a *Web Application*, *managed path* or *site collection*.
3. On the **Commands** Ribbon tab, click the **Audit Permissions** split button down arrow and then click **Alert Me**.

The **Operation: Alerts Management** page is displayed in the results pane of the DeliverPoint dashboard. Existing Alerts for the SharePoint objects selected are listed on this page.

4. If you have selected the **Server Farm**, *Web Application*, *Managed Path* or site collection_ to see Alerts created for sites within these scopes, select the **Include Child Scopes** checkbox.
5. Use the filter  icon to the left of the column heading to display the **Filter By Creation/Modification Date** dialog, which you can use to set criteria so only a subset of alerts are displayed.
6. To modify an alert, click the Edit  icon to the right of the alert to display the **Edit Alert** dialog.


Reviewing alerts

To review alerts, complete the following steps:

1. Click **Settings**  and then click **DeliverPoint 2013** to display the [DeliverPoint dashboard](#), ensure the [Farm Centric view](#) is selected.
2. In the tree view, select the checkbox to the left of the SharePoint object where the alert was created. If you select more than one SharePoint object then alerts for all those objects are displayed. If you are unsure where alerts have been created, click **Server Farm**, a *Web Application*, *managed path* or *site collection*.
3. On the **Commands** Ribbon tab, click the **Audit Permissions** split button down arrow and then click **Alert Me**.
The Operation: Alerts Management page is displayed in the results pane of the DeliverPoint dashboard. Existing Alerts for the SharePoint objects selected are listed on this page.
4. If you have selected the **Server Farm**, *Web Application*, *Managed Path* or site collection_ to see Alerts created for sites within these scopes, select the **Include Child Scopes** checkbox.
5. Use the filter  icon to the left of the column heading to display the **Filter By Creation/Modified Date** to display a subset of alerts.
6. To review the details of an alert, click the Edit  icon to the right of the alert to display the **Edit Alert** dialog.


Delete an alert

To delete an alert, complete the following steps:

1. Click **Settings**  and then click **DeliverPoint 2013** to display the [DeliverPoint dashboard](#), ensure the [Farm Centric view](#) is selected.
2. In the tree view, select the check box to the left of the relevant SharePoint object where the alert was created. If you are unsure where alerts have been created, click **Server Farm**, a *Web Application*, *managed path* or *site collection*.

3. On the **Commands** Ribbon tab, click the **Audit Permissions** split button down arrow and then click **Alert Me**.

The Operation: Alerts Management page is displayed in the results pane of the DeliverPoint dashboard. Existing Alerts for the SharePoint objects selected are listed on this page.

4. If you have selected the **Server Farm**, *Web Application*, *Managed Path* or site collection_ to see alerts created for sites within these scopes, select the **Include Child Scopes** check box.
5. To the left of the alert, click the delete  icon to delete the alert.

[<< Tracking Permission Changes](#)


[Auditing >>](#)

Auditing

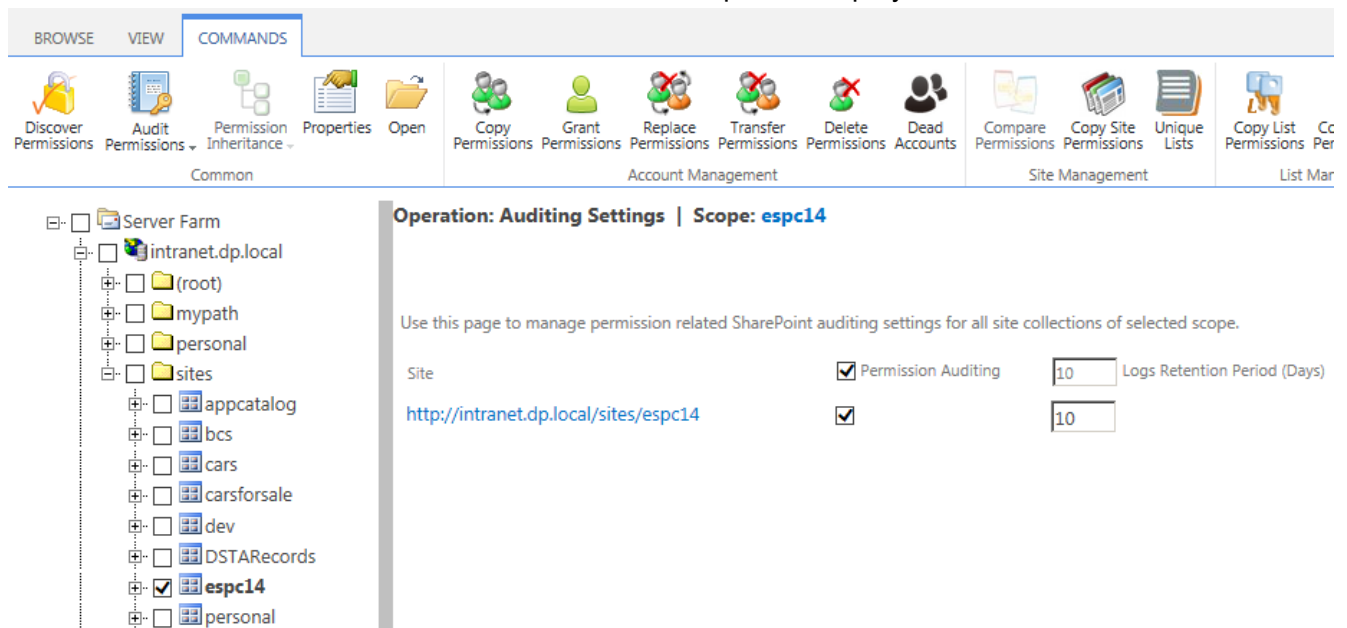
You can audit permission changes using DeliverPoint.

Enabling auditing

To configure auditing, complete the following steps:

1. Click **Settings**  and then click **DeliverPoint 2013** to display the [DeliverPoint dashboard](#), ensure the [Farm Centric view](#) is selected.
2. In the tree view, select the checkbox to the left of one or more Web Application, Managed Paths or site collections.

The **Operation: Audit Settings** page is displayed in the results pane of the [DeliverPoint dashboard](#). A list of the site collections included in the selected scope are displayed.



Operation: Auditing Settings | Scope: espc14

Use this page to manage permission related SharePoint auditing settings for all site collections of selected scope.


Site	Permission Auditing	Logs Retention Period (Days)
http://intranet.dp.local/sites/espc14	<input checked="" type="checkbox"/>	<input type="text" value="10"/>

3. Select or de-select site collections which you wish to audit and specify the number of days to retain the audit logs for that site collection.

Note: Auditing, can only be configured at a site collection level.

Removing permission auditing

To remove permission auditing:

1. Click **Settings**  and then click **DeliverPoint 2013** to display the [DeliverPoint dashboard](#), ensure the [Farm Centric view](#) is selected.
2. In the tree view, select the checkbox to the left of the Web Application, Managed Paths that contains the site collections or select the check box for the site collection.
The **Operation: Audit Settings** page is displayed in the results pane of the [DeliverPoint dashboard](#).
A list of the site collections included in the selected scope are displayed.
3. Deselect the check box to the right of the site collection.

Viewing auditing reports

To view the auditing reports:

1. Use [DeliverPoint dashboard](#) treeview to select the site collection or a site within the site collection.
2. Click the **Audit Permission** button on the **Commands** tab to produces a report for the number of days the audit logs have been retained.

BROWSE

COMMANDS

Discover Permissions

Audit Permissions

Copy Permissions

Grant Permissions

Replace Permissions

Transfer Permissions

Delete Permissions

Permission Inheritance

Export to Spreadsheet

View Scope

Changes Via Parent

Online Documentation

Help

Permission Management

Reporting

Display Options

Links

Lists

Home

Documents

Subsites

Di-Data

Recent

Tasks

Site Contents

EDIT LINKS

Show Changes After

5/1/2015

Show Changes Until

5/8/2015

Permission Changes

Date	Initiator	Scope	Changed Via	Permission	+/-	Member
<input type="checkbox"/> 5/5/2015 4:50:08 PM	SHAREPOINT\system	ESPC14	ESPC14	All Roles		Bills Group
<input type="checkbox"/> 5/5/2015 4:50:08 PM	SHAREPOINT\system	Business Connectivity Services	ESPC14	All Roles		Bills Group
<input type="checkbox"/> 5/5/2015 4:50:08 PM	SHAREPOINT\system	OracleJobs	ESPC14	All Roles		Bills Group
<input type="checkbox"/> 5/5/2015 4:50:08 PM	SHAREPOINT\system	Salesforce BCS	ESPC14	All Roles		Bills Group
<input type="checkbox"/> 5/5/2015 4:50:08 PM	SHAREPOINT\system	SPTechCon2015_Austin_BCS	ESPC14	All Roles		Bills Group
<input type="checkbox"/> 5/5/2015 4:50:08 PM	SHAREPOINT\system	Television Sales	ESPC14	All Roles		Bills Group
<input type="checkbox"/> 5/5/2015 4:50:08 PM	SHAREPOINT\system	Data Viewer	ESPC14	All Roles		Bills Group
<input type="checkbox"/> 5/5/2015 4:50:08 PM	SHAREPOINT\system	Rollup	ESPC14	All Roles		Bills Group
<input type="checkbox"/> 5/5/2015 4:50:08 PM	SHAREPOINT\system	Hitachi	ESPC14	All Roles		Bills Group
<input type="checkbox"/> 5/5/2015 4:50:08 PM	SHAREPOINT\system	Lightning Conductor Training	ESPC14	All Roles		Bills Group
<input type="checkbox"/> 5/5/2015 4:50:08 PM	SHAREPOINT\system	Lightning Conductor Webinar	ESPC14	All Roles		Bills Group
<input type="checkbox"/> 5/5/2015 4:50:08 PM	SHAREPOINT\system	Sales	ESPC14	All Roles		Bills Group
<input type="checkbox"/> 5/5/2015 4:50:08 PM	SHAREPOINT\system	SUGUK Vendor Night	ESPC14	All Roles		Bills Group
<input type="checkbox"/> 5/5/2015 4:50:08 PM	SHAREPOINT\system	Training	ESPC14	All Roles		Bills Group
<input type="checkbox"/> 5/5/2015 4:50:08 PM	SHAREPOINT\system	Lightning Conductor Webinar	ESPC14	All Roles		Bills Group

The audit report displays which group members have been added or removed and users and / or groups that have been deleted. The person who performed the permission change, and when the change occurred are also displayed.

[<< Alerts](#)

[Permission Inheritance >>](#)

Permission Inheritance

“Inherit / disinherit permission from parent site”

For easier administration, it is recommend that you avoid breaking [inheritance](#) too frequently, that is, you should keep the permissions inheritance intact for all sites, lists, libraries, and items. To avoid breaking inheritance at the list / library / list item or file level, you should organize sites so that you can assign permissions to the site that contains the protected content. For example, you might create a sub site for documents that contain sensitive data, or a sub site that contains lists with restricted access. In this way, you can manage permissions for all content in a site with one action, instead of tracking many individual documents or list items. See the white paper, [Best practices for using fine-grained permissions](#).

If you believe permission inheritance has been broken at the list, library, list item or file levels, then you can use the [Unique Lists](#) and [Unique Items](#) DeliverPoint commands to find where permission inheritance was stopped and different permissions assigned. You can also add a column a list / library, based on the [DeliverPoint inheritance field](#) to display folder, list item, file permission inheritance in views.



Note: A site collection is a security boundary, that is, the top-level site of the site collection, does not inherit its permission settings from any other site. The site collection administrator configures the initial permissions settings for a site collection, which are then inherited by the content in the site collection (sites, lists, libraries, list items and files).

You can use DeliverPoint to manage site, list, folder or item-level permission inheritance. You can use the **Permission Inheritance** DeliverPoint commands, from the [DeliverPoint dashboard](#) or by navigating to the list / library where you want to manage permission inheritance.

To use the [DeliverPoint dashboard](#), complete the following steps:

1. Navigate to the [DeliverPoint dashboard](#) and using the **View** Ribbon tab, click either the [Farm Centric](#) or [Account Centric](#).
2. In the tree view, select those sites to be included in the scope. If [lists and libraries are displayed in the tree view](#), you can also select a list or library. The *Permission Inheritance* commands can not be used on an accounts. The properties of the node selected are displayed in the dashboard's **Properties** pane.

On the **Commands** Ribbon tab, click **Permission Inheritance** and then click either **Inherit**

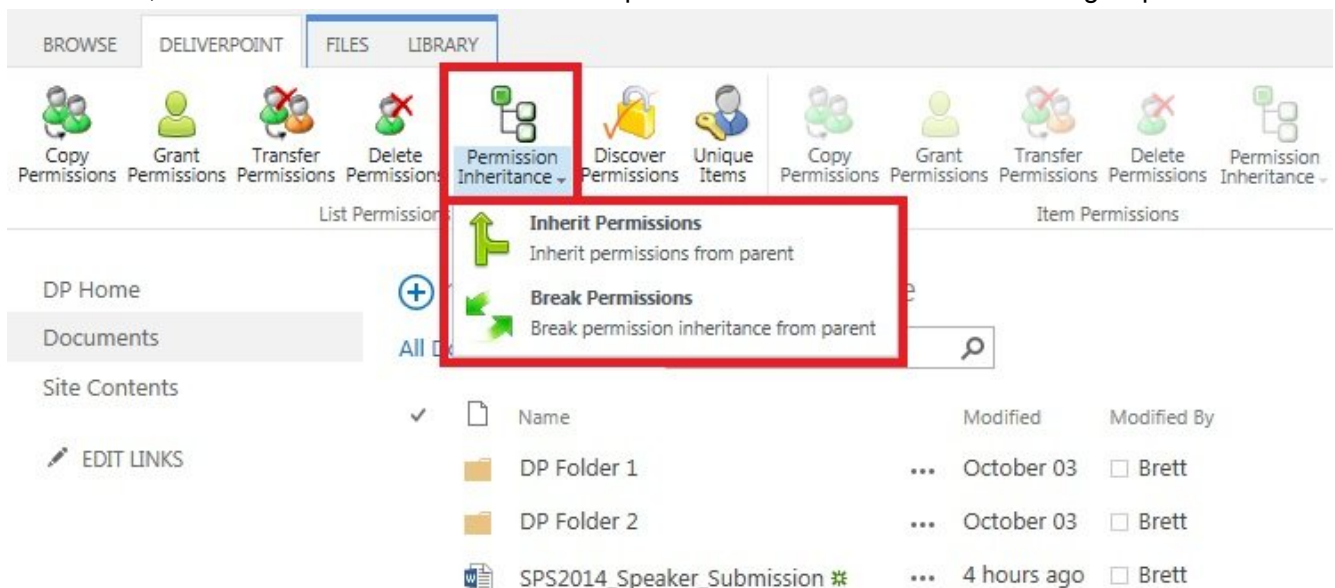
Permissions or Break Permissions.



Note: When you select *Inherit Permissions*, you will lose any unique permission settings that you have configured on that site.

To use the *Permissions Inheritance* commands on a list, library, folder, list item or file, complete the following steps:

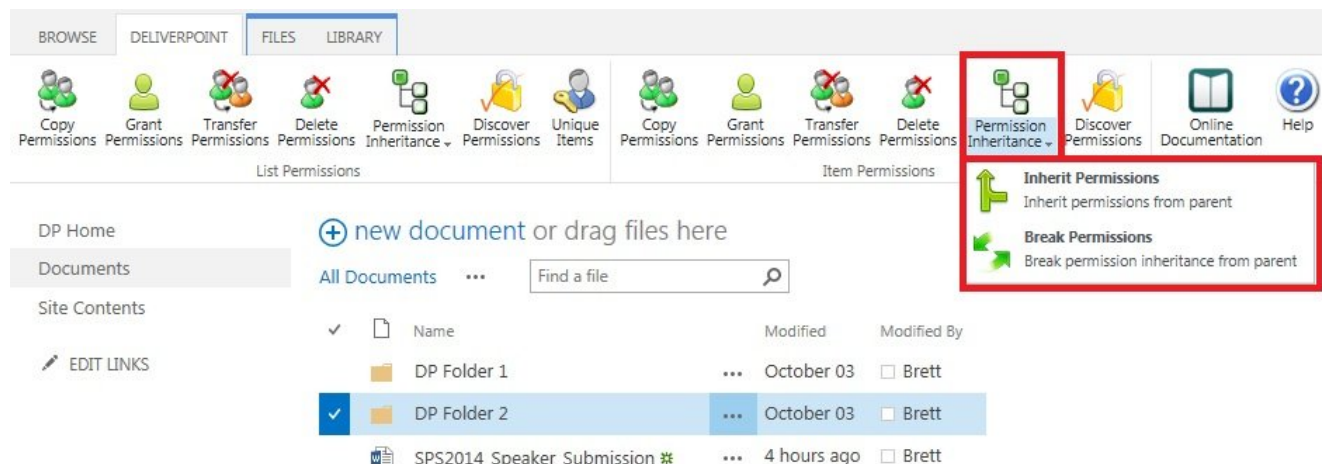
1. Navigate to the list where you want to use the DeliverPoint *Permission Inheritance* commands.
2. When you wish to use the Permission Inheritance commands on a list, then on the **DeliverPoint** Ribbon tab, click the **Permission Inheritance** split button in the **List Permissions** group.



3. When you wish to use the Permission Inheritance commands on a folder, item or file:

- Click to the left of the folder, list item or file.

- On the **DeliverPoint** Ribbon tab, click **Permission Inheritance** split button in the **Item Permissions** group.



The *Break Permissions Inheritance* or *Inherit Permissions* page is displayed. The scope of the operation is display.

Break Permissions Page

Scope: Documents

Operation will break permission inheritance for selected objects.

☒ Keep Role Assignments

Break

- When you select to *Break Permission* command you can choose to clear the **Keep Role Assignments** check box if required. By default, this check box is selected and therefore the permission configuration is the same as it was before. When the check box is cleared, then the previously inherited permission configuration is not copied.

- Click **Break** or **Inherit**.

The *Operation completed successfully* page is displayed.

Break Permissions Page

Scope: Documents

Operation completed successfully. NOTE: After performing this action, the DeliverPoint interrogation will need to run to update the inheritance status of this object(s).

- ✿ To avoid confusion or future inaccuracies, LightningTools recommend that before completing any other permission-related tasks to the sites you targeted with the *DeliverPoint Permission Inheritance* action, you wait for the next time the DeliverPoint SharePoint Interrogation timer job is scheduled to run or you ask your SharePoint server administrator to run the timer job.

References

[Best practices for using fine-grained permissions](#)

Related DeliverPoint commands and functionality:

- [Discover Permissions](#)
- [Unique Permissions](#)
- [Unique Lists Detection](#)
- [Unique Item Detection](#)
- [Inheritance Field](#)

[<< Auditing](#)

[Properties >>](#)

Properties

“Monitor farm growth.”

DeliverPoint 2013 provides introductory statistics on your farm, allowing you to understand the aggregate total, age and size of web applications, managed paths, site collections, webs, and lists within your farm. Using DeliverPoint 2013, you can objectively define the following categories as they relate to the aforementioned SharePoint objects:

- Small
- Medium
- Large
- New
- Aging
- Old


✿ The thresholds for these categories can be modified by a SharePoint server administrator using the [DeliverPoint configuration](#) page in the SharePoint 2013 Central Administration web site, and then by clicking [Threshold Settings](#).

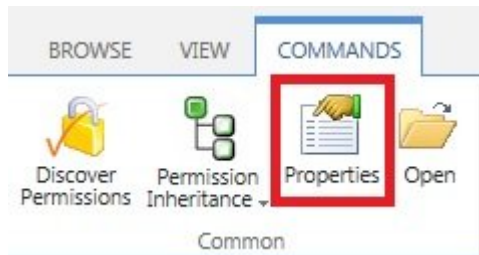
These categories can then be used to segment your farm, web application, managed path, site collection, or web's statistical information. For example, you can define that a “large” list is a list that has over 200 MB of information or that a list that is older than 105 days is “aging”. Once defined, DeliverPoint tells you how many “large” and “aging” lists you have at any scope within your farm. You can view size and aging information for any object as previously described.

✿ The Properties action can only be used by [DeliverPoint:permissions operators](#) and site collection administrators. You can not use the properties command in the [Account Centric View](#).

To use the **Properties** command, complete the following steps:

1. Click **Settings**  and then click **DeliverPoint 2013** to display the [DeliverPoint dashboard](#).

- Click the plus sign (+) to the left of a Web Application , and continue to click the plus signs to expand the objects under the Web Application, until you are able to select the SharePoint object you wish to see the properties. When a SharePoint object is selected a summary of the object's properties are displayed in the dashboard's *Properties* pane.
- On the **Commands** Ribbon tab, click **Properties** in the **Common** group.





The *Properties* page is displayed in the dashboard results pane.

Demos Web Properties

Aggregate Data

	New	Aging	Old	Empty	Small	Medium	Large
Sites (1)	0	0	1	0	0	0	1
Subsites (27)	0	1	26	0	24	1	2
Lists (243)	0	17	226	6	230	5	2

This page displays **Aggregate Data**. When you select a site collection , the data is aggregated for the site collection, site and list information. When you select a site , then the aggregated data is site, subsites, and lists. The SharePoint objects are classified into **New**, **Aging**, **Old**, **Empty**, **Small**, **Medium** and **Large** categories.

- You can save the report. On the **Report** Ribbon tab, click **Export to Spreadsheet** in the **Actions** group. The Microsoft® Excel spreadsheet file name is of the format, *Properties_yyyymmdd.xls*.
- When you select a site collection you can display usage information in the dashboard results pane, by clicking **Display Usage Information**, which is a link above the *Aggregate Data* section.

LT Site Collection Properties

Attributes

Content Database Name:	WSS_Content_ecc2b17fcf894768bbe6aeb9af399756
Host Name:	intranet.dp.local
Port:	80
Portal Name:	Intranet
Owner:	administrator
Secondary Contact:	
Storage Maximum:	0 bytes
Storage Warning Level:	0 bytes
Zone:	Default
Read Locked:	No
Read Only:	No
Write Locked:	No

[Display Usage Information](#)

Aggregate Data

Additional information is displayed in the results pane, that you could use to clean up content from your site(s) by deleting the large content that is no longer needed.

LT Site Collection Properties

Actions ▾

Usage Information

Storage Used:	10456099 bytes
Discussion Storage Used:	0 bytes

Recycle Bin (Manage Recycle Bin)

Item Count:	2
Size:	10811 bytes

Largest Lists

Name	Location	Size (bytes)	Last Modified
Reporting Metadata	divisions/LT/Lists	79927	2/7/2014 11:52:00 AM
Tasks	divisions/LT/Lists	61801	2/13/2014 4:28:00 PM
Tasks	divisions/LT/LCWP/Lists	61615	2/13/2014 4:29:00 PM
Tasks	divisions/LT/DP/Lists	61449	4/16/2014 2:25:00 PM
Tasks	divisions/LT/SS/Lists	61449	3/21/2014 2:39:00 PM
Calendar	divisions/LT/Lists	52319	2/11/2014 3:29:00 PM
Team Discussion	divisions/LT/Lists	51889	2/11/2014 3:29:00 PM

This results pane contains the following information:

- **Storage Used.** This is the amount of data used by all content within the site collection. This is useful when your site collection is associated with a [quota](#).
- **Discussion Storage Used.** This is storage used for [Web discussion](#), a special collaboration feature that allowed users to collaborate on HTML documents or on any document that can be opened with a browser (such as .htm, .xls, .doc, and .ppt files). This feature is very rarely used and on most SharePoint installations, the value will be 0 bytes.
- **Recycle Bin.** A link to the [Site Collection Administration Recycle Bin](#) page, an Item Count of the number of items in the Recycle Bin, and the Size of the items in the Recycle Bin.
- **Largest Lists.** Sort in descending order, this section contains the name of the list, its location, size in bytes, and the date and time the list was last modified.
- **Largest Document Libraries.** Sort in descending order, this section contains the name of the list, its location, size in bytes, and the date and time the list was last modified.
- **Largest Documents.** Sort in descending order, this section contains the name of the file, its location, size in bytes, and the date and time the list was last modified.
- **Aggregate Data.** This section was documented previously on this page.

References

[<< Permission Inheritance](#)
[Account Management >>](#)

Account Management

[DeliverPoint 2013](#) allows you to manage SharePoint permissions in Microsoft® SharePoint® Server 2013 or Microsoft® SharePoint Foundation 2013 on-premises deployments. From the tree view on the [DeliverPoint dashboard](#) by clicking a SharePoint object you can initiate DeliverPoint tasks, which are displayed on the Commands Ribbon tab and divided into the Ribbon groups, **Common**, **Account Management**, [Site Management](#) and [List Management](#) commands. The **Account Management** actions you can complete are listed below.

✿ Note, not all actions can be completed on all SharePoint objects.

- [Copy Permissions](#)
- [Grant Permissions](#)
- [Transfer Permissions](#)
- [Delete Permissions](#)
- [Dead Account Detection](#). This action is available for the following scopes, farm and site collection,
- [Unique Permissions](#). This action can only be used when using the [Accounts Centric View](#).

The [Copy](#), [Delete](#), and [Transfer Permissions](#) actions can use [Active Directory](#) user or group accounts along with [Forms Based Authenticated](#) (FBA) users and [Claims Based Authenticated](#) users. You cannot copy a SharePoint Group's permissions. Instead, you can copy any account within a SharePoint Group to any other account, whether it's in a SharePoint Group or not.

References

- [← DeliverPoint dashboard](#)
- [Site Management →](#)

Copy Permissions

“Copy an account’s permissions to another account”

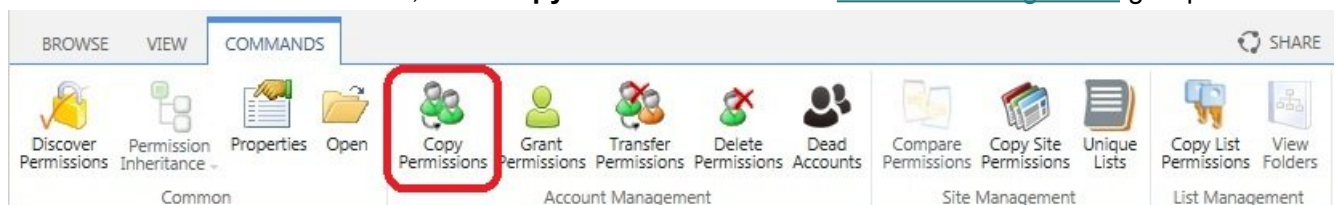
When you choose to use the **Copy Permissions** command, changes will be applied to all sites, lists, folders and list items in the select scope(s), where you are able to manage SharePoint permissions. If you are not able to manage permissions for a specific site, folder, list or list item, changes will not be applied to that object.

✳ DeliverPoint will not at any time enumerate membership of an Active Directory group during the **Copy Permissions** operation.

The source permission rights are appended to the existing permissions for the target account(s). The effect of appending permission rights is that none of the existing permissions for the target account(s) are replaced or deleted. Instead, the permissions are given to the target account in addition to existing permissions. For example, if the target account has **Read** permissions on *Site A* and the source account has **Contribute** permissions on *Site A*, then the target account’s permissions in *Site A* will now include **Contribute**. However, if in *Site B* the target account’s permissions are **Design** and the source account’s permissions are **Read**, then the target account’s permission will retain the higher permission level of **Design** while still receiving the new **Read** permission level. In other words, permissions are appended and not replaced in the copy operation.

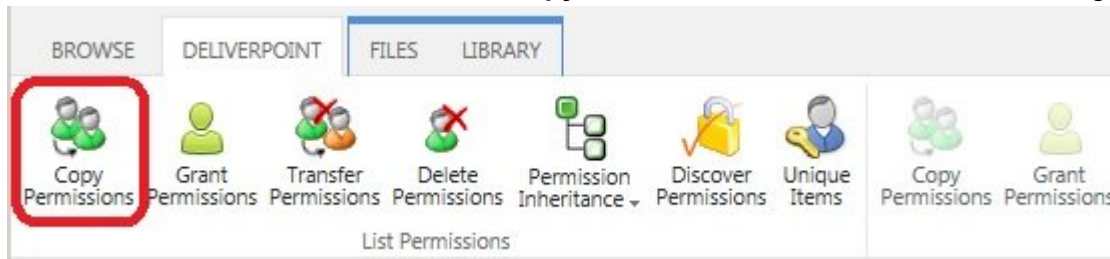
To use the **Copy Permissions** command, either:

1. Navigate to the [DeliverPoint dashboard](#), use the **View** Ribbon tab, click either the [Farm Centric](#) or [Account Centric](#).
2. In the tree view, select those nodes, also known as SharePoint objects, to be included in the scope, for example, one or more site collections, sites or an accounts. The properties of the node selected are displayed in the dashboard’s **Properties** pane.
Note: Child nodes are not automatically included.
3. On the **Commands** Ribbon tab, click **Copy Permissions** in the [Account Management](#) group.



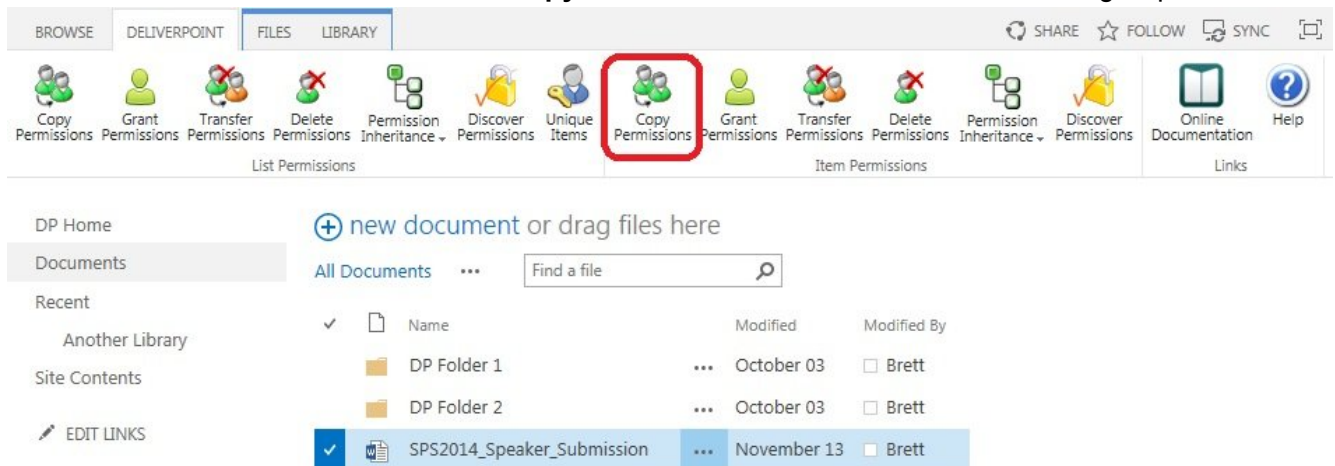
or

1. Navigate to the list or library that you want to use as the source for your copy permission.
2. On the **DeliverPoint** Ribbon tab, click **Copy Permissions** in the **List Permissions** group.



or

1. Navigate to the list or library where you want to copy permission on items or files.
2. On the **DeliverPoint** Ribbon tab, click **Copy Permissions** in the **Item Permissions** group.



The **Operation: Copy Permissions / Clone Permissions** page is displayed. The nodes included in the scope are display on this page.




1. Complete information in the following sections. You may need to scroll down to see all the sections:
 - **Copy Permission From.** Use this section to identify the source usernames, groups or email address of the account (source) you wish to use as a basis for the copy operation.
 - From the drop down list, select either **User or Domain Group** or **SharePoint Group**.

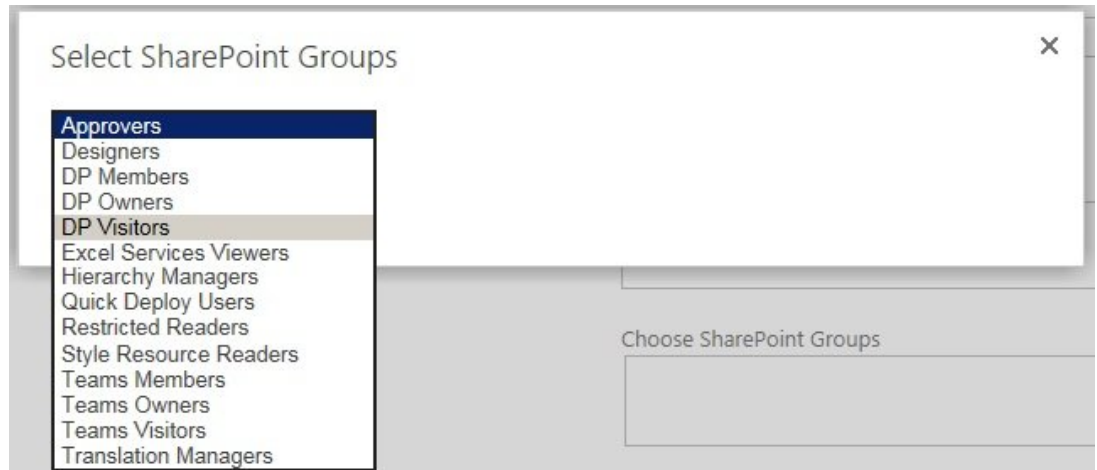
Copy Permissions From



You can enter a username, domain group name, e-mail address or SharePoint group name.

User or Domain Group
SharePoint Group



- When *User or Domain Group* is selected, you can use either:
 - The **Browse**  icon to select the source username/ Active Directory groups, or
 - In the people picker text box, type usernames, groups or email address separated by a semi colon (;), and then click the **Check Names**  icon to verify that you have typed valid usernames.
- When *SharePoint Group* is selected you can use the **Browse**  icon to display the **Select SharePoint Groups** dialog.
 - Select a *SharePoint Group* from the drop down list.



- Click **OK** to close the dialog.
- **Copy Permissions To.** Use this section to identify the target usernames, email address, Active Directory groups or SharePoint Groups. You can use either
 - The **Browse**  icon to the right of either the **Choose Users or Domain Groups** text box or the **Choose SharePoint Groups** text box to select the target username/groups, or
 - In the people picker text box, type usernames, groups or email address separated by a semi colon (;), and then click the **Check Names**  icon to verify that you have typed valid usernames.

Use this page to configure a copy permissions job. Changes will be applied to all sites, lists, folders, and list items within scope.

Copy Permissions From

You can enter a username, domain group name, e-mail address or SharePoint group name.

User or Domain Group 

Brett



Copy Permissions To

You can enter usernames, domain group names, e-mail addresses or SharePoint group names. Separate them with semicolons.

Choose Users or Domain Groups

Zoe; Andy Carter



Choose SharePoint Groups



- **Job Processing.** Select one of the [transaction types](#): **Run Now**, **Run Later** or **Both**. This option determines when the job will be processed. The default setting is **Both**.

Job Processing

Select when this job will be performed.

☒ Run Now 

☐ Run Later 

☐ Both 

- **Options.** Select or deselect the check box, **Alerts**. According to the permissions of the current user, alerts can be chosen to be included or not. For more information, see [Security Trimming](#).

Options

Select additional options.

Include:

☒ Alerts

- Click **Next** to display the confirmation screen.

Use this page to confirm copy permissions job.

Verify "Copy From" member	
This member's permissions will be copied.	DP\brett
Verify "Copy To" members	
The copied permissions will be appended to these members.	DP\zoe DP\andy


Note: Requested changes will be made only to sites, folders, lists, and list items where you are able to manage SharePoint permissions. If you are not able to manage permissions for a specific site, folder, list, or list item, changes will not be applied to that object.

- Review and then click **OK**. The page then displays that the Jobs have been successfully created. This page does not mean that the *Copy Permissions* DeliverPoint command is complete. If you choose the transaction type: *Both*, then two DeliverPoint jobs will be created. The *Copy Permissions* command will not be processed until the DeliverPoint job is completed. DeliverPoint executes the job according to the timing of the [Transaction Type](#) selected.

Jobs have been successfully created to copy the selected member's permissions.

[Return](#) | [Job Status](#)

- Click **Return** to display the **Operation: Copy Permissions / Clone Permissions** page so you can complete another **Copy Permissions** action, or click **Job Status** to display the [DeliverPoint Job Status and History](#) page, which you can use to monitor the Copy Permissions DeliverPoint job(s).

 **Note:** You can display the [DeliverPoint Job Status and History](#) page from the **View** Ribbon tab on the [DeliverPoint dashboard](#).

References

[<< Account Management](#)
[Grant Permissions >>](#)

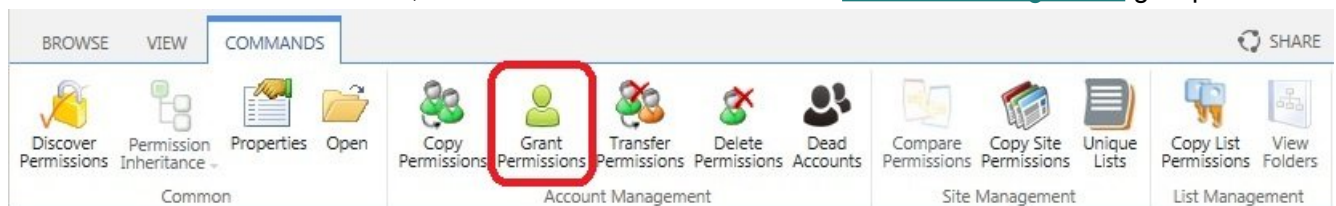
Grant Permissions

“Grant Permissions to a specific account.”

Using this DeliverPoint permission command, you can grant permissions at a SharePoint object level, such as a site collection, site, list, library, list item, file to one or more usernames, email addresses, Active Directory groups or SharePoint groups, or a combination, which you then map to a permission level or SharePoint Group.

To use the **Grant Permissions** command, complete one of the three following methods:

1. Navigate to the [DeliverPoint dashboard](#) and using the **View** Ribbon tab, select either the [Farm Centric](#) or [Account Centric](#).
2. In the tree view, select those nodes, also known as SharePoint objects, to be included in the scope, for example, one or more site collections, sites or an accounts. The properties of the node selected are displayed in the dashboard's **Properties** pane.
Note: Child nodes are not automatically included.
3. On the **Commands** Ribbon tab, click **Grant Permissions** in the [Account Management](#) group.



or



1. Navigate to the list or library that you want to use as the source for your grant permission.
2. On the **DeliverPoint** Ribbon tab, click **Grant Permissions** in the **List Permissions** group.

or

1. Navigate to the list or library that contain list items/files whose permission setting you want to use as the source for your grant permission.
2. On the **DeliverPoint** Ribbon tab, click **Grant Permissions** in the **Item Permissions** group.

The **Grant Permissions** page is displayed. The nodes included in the scope are displayed on the page.

1. Complete information in the following sections. You may need to scroll down to see all the sections:

- **Grant Permissions To.** Use this section to identify the target usernames, Active Directory groups, SharePoint Groups or email address of the account (source) you wish to use as a basis for the copy operation. You can use either:
 - The **Browse**  icon to select the source username/groups, or
 - In the people picker text box, type usernames, Active Directory groups or email addresses and then click the **Check Names**  icon to verify that you have typed valid usernames.

Grant Permissions To

You can enter a usernames, domain group names, e-mail addresses or SharePoint group names.

Choose Users or Domain Groups

Brett; Zoe; DP\g_sales



Choose SharePoint Groups

DP Members



- **Permissions.** Use this section to select the permission level(s). The permission levels that are displayed in this section are dependant on the permission levels defined for your scope.

Permissions

Select permissions to be granted

Grant:

- ☐ AllowCreateEXT
- ☐ Approve
- ☐ Contribute
- ☒ Design
- ☐ Edit
- ☐ Full Control
- ☐ Manage Hierarchy
- ☐ Read
- ☐ Restricted Interfaces for Translation
- ☐ Restricted Read
- ☐ View Only

- **Groups.** Use this section to add SharePoint Groups that the accounts must be added to in order to grant permissions. Use the **Browse**  icon to display the **Select SharePoint Groups**

dialog, which you can use to select one or more *SharePoint Groups*.

Groups

Select groups to which the accounts must be added in order to grant permissions

Add users to Groups:

Designers; Teams Members



- **Grant Duration.** Use this option to temporarily grant permissions to a user or group. Measurement is in minutes allowing you to assign permissions for a period of time to perform a specific job, or for a contractor that is employed for a temporary period. After the expiration, the permissions will be revoked.

Grant Duration

Specify duration in minutes after which granted permissions will be automatically revoked.

Duration in minutes

- **Job Processing.** Select one of the [transaction types](#): **Run Now**, **Run Later** or **Both**. This option determines when the job will be processed. The default setting is **Both**.

Job Processing

Select when this job will be performed.

☒ Run Now

☐ Run Later

☐ Both

- **Options.** Select or deselect the check boxes:
 - **Process Subwebs**
 - **Process Lists**
 - **Process List/Folder Items**

7. Click **Next** to display the confirmation screen in the results pane.

Use this page to confirm the grant permissions job.

Verify "Grant To" members

Permissions will be granted to these members.

DP\brett
DP\zoe
DP\g_sales
DP Members

Verify selected permissions

These permissions will be granted to members.

Design

Verify selected groups

Permissions of accounts will be granted via these groups.

Designers
Teams Members

Note: Requested changes will be made only to sites, folders, lists, and list items where you are able to manage SharePoint permissions. If you are not able to manage permissions for a specific site, folder, list, or list item, changes will not be applied to that object.

OK

Cancel

8. Review and then click **OK**. The *Grant Permissions* page is displayed, stating that the jobs have been successfully created. This page does not mean that the *Grant Permissions* DeliverPoint command is complete. The *Grant Permissions* command will not be complete until the DeliverPoint jobs are completed. DeliverPoint executes the jobs according to the timing of the [Transaction Type](#) selected.
9. Click **Return** to display the *Grant Permissions* page so you can complete another **Grant Permissions** command, or click **Job Status** to display the [DeliverPoint Job Status and History](#) page, which you can use to monitor the *Grant Permissions* DeliverPoint job(s).



Note: You can display the [DeliverPoint Job Status and History](#) page from the **View** Ribbon tab on the [DeliverPoint dashboard](#).

References

[<< Copy Permissions](#)

[Transfer Permissions >>](#)

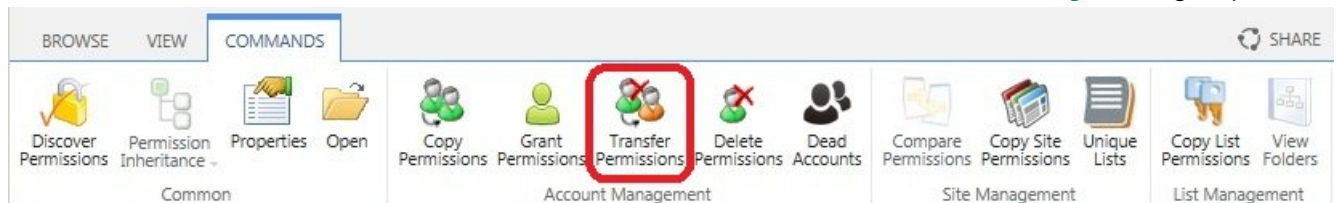
Transfer Permissions

“Move an account’s permissions to another account”

DeliverPoint allows you to select a scope, copy the permission set of an account (source) within that scope to other account(s) (target), and then the source account is deleted within the selected scope. This operation is a combination of the [Copy Permissions](#) and [Delete Permissions](#) commands.

To use the **Transfer Permissions** command, complete one of the following three methods:

1. Navigate to the [DeliverPoint dashboard](#) and using the **View** Ribbon tab, select either the [Farm Centric](#) or [Account Centric](#).
2. In the tree view, select those nodes, also known as SharePoint objects, to be included in the scope, for example, one or more site collections, sites or an accounts. The properties of the node selected are displayed in the dashboard’s **Properties** pane.
Note: Child nodes are not automatically included.
3. On the **Commands** Ribbon tab, click **Transfer Permissions** in the [Account Management](#) group.



or

1. Navigate to the list or library that you want to use as the source for your transfer permission.
2. On the **DeliverPoint** Ribbon tab, click **Transfer Permissions** in the **List Permissions** group.

or

1. Navigate to the list or library that contain list items/files whose permission setting you want to use as the source for your transfer permission.
2. On the **DeliverPoint** Ribbon tab, click **Transfer Permissions** in the **Item Permissions** group.

The **Transfer Permissions** page is displayed. The nodes included in the scope are display to the right of the page title.

1. Complete information in the following sections. You may need to scroll down to see all the sections:

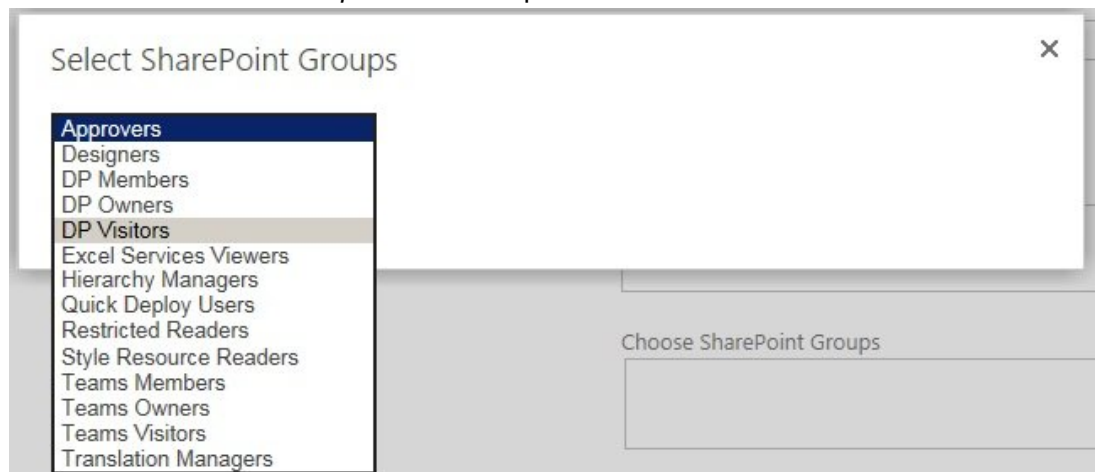
- **Transfer Permissions From.** Use this section to identify the source usernames, groups or email address of the account (source) you wish to use as a basis for the transfer operation. The source account is the account from which the permissions are to be copied from, and the account to be subsequently deleted.

- From the drop down list, select either **User or Domain Group** or **SharePoint Group**.

Copy Permissions From

You can enter a username, domain group name,
e-mail address or SharePoint group name.

- When *User or Domain Group* is selected, you can use either:
 - The **Browse** icon to select the source username/ Active Directory groups, or
 - In the people picker text box, type usernames, groups or email address separated by a semi colon (;), and then click the **Check Names** icon to verify that you have typed valid usernames.
- When *SharePoint Group* is selected you can use the **Browse** icon to display the **Select SharePoint Groups** dialog.
 - Select a *SharePoint Group* from the drop down list.



- Click **OK** to close the dialog.

Note Only one username, Active Directory group or SharePoint Group can be specified.

- **Transfer Permissions To.** Use this section to identify one or more the target usernames, Active Directory groups, SharePoint Groups or email address or a combination. The target account(s) is the account to whom the permissions will be copied to. DeliverPoint 2013 allows multiple target accounts to be added in one job. You can use either
 - The **Browse** icon to select the target username/groups, or
 - In the people picker text box, type usernames, Active Directory groups or email address separated by a semi colon (;), and then click the **Check Names** icon to verify that you have typed valid usernames.

Transfer Permissions To

You can enter usernames, domain group names, e-mail addresses or SharePoint group names. Separate them with semicolons.

Choose Users or Domain Groups

Zoe; DP\g_sales

**Choose SharePoint Groups**

Teams Members



- **Job Processing.** Select one of the [transaction types](#): **Run Now**, **Run Later** or **Both**. This option determines when the job will be processed. The default setting is **Both**.

Job Processing

Select when this job will be performed.

☒ Run Now

☐ Run Later

☐ Both

- **Options.** Select or deselect the check box, **Alerts**. According to the permissions of the current user, alerts can be chosen to be included or not. For more information, see [Security Trimming](#).

5. Click **Next** to display the confirmation screen.

Use this page to confirm transfer permissions job.

Verify "Transfer From" member

This member's permissions will be copied, then deleted (transferred).

DP\brett

Verify "Transfer To" members

The transferred permissions will be appended to these members.


DP\zoe
DP\g_sales
Teams Members

Note: Requested changes will be made only to sites, folders, lists, and list items where you are able to manage SharePoint permissions. If you are not able to manage permissions for a specific site, folder, list, or list item, changes will not be applied to that object.

OK

Cancel

6. Review and then click **OK**. The *Transfer Permissions* page is displayed stating that the DeliverPoint jobs have been successfully created. This page does not mean that the *Transfer Permissions* DeliverPoint command is complete. If you choose **Both**, for the [Transaction Type](#), then two jobs will be created a **Run Now** and a **Run Later** job. The *Transfer Permissions* command will not be complete until the related DeliverPoint job(s) are completed.
7. Click **Return** to display the *Transfer Permissions* page, or click **Job Status** to display the [DeliverPoint Job Status and History](#) page, which you can use to monitor when the two DeliverPoint jobs are completed.

 **Note:** You can display the [DeliverPoint Job Status and History](#) page from the **View** Ribbon tab on the [DeliverPoint dashboard](#).

References

[<< Grant Permissions](#)

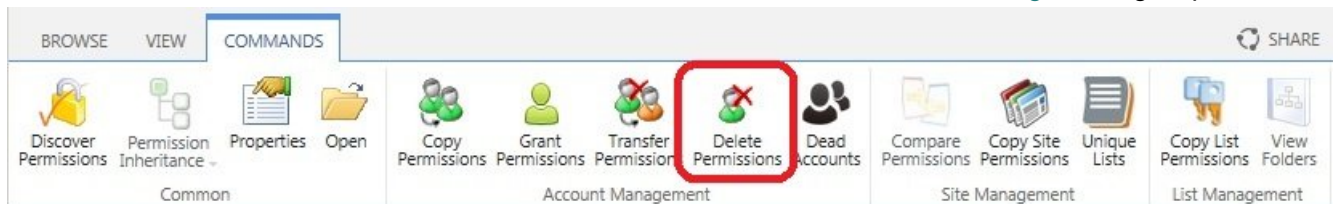
[Delete Permissions >>](#)

Delete Permissions

“Delete an account’s permissions”

To use the **Delete Permissions** command, complete one of the following three methods:

1. Navigate to the [DeliverPoint dashboard](#) and using the **View** Ribbon tab, select either the [Farm Centric](#) or [Account Centric](#).
2. In the tree view, select those nodes, also known as SharePoint objects, to be included in the scope, for example, one or more site collections, sites or an accounts. The properties of the node selected are displayed in the dashboard’s **Properties** pane.
Note: Child nodes are not automatically included.
3. On the Commands Ribbon tab, click **Delete Permissions** in the [Account Management](#) group.



or



1. Navigate to the list or library that you want to use as the source for your delete permission.
2. On the **DeliverPoint** Ribbon tab, click **Delete Permissions** in the **List Permissions** group.

or

1. Navigate to the list or library that contain list items/files whose permission setting you want to use as the source for your delete permission.
2. On the **DeliverPoint** Ribbon tab, click **Delete Permissions** in the **Item Permissions** group.

The **Delete Permissions** page is displayed in the dashboard results pane. The nodes included in the scope are display to the right of the page title.

1. Complete information in the following sections. You may need to scroll down within the results pane to see all the sections:

- **Delete Permissions From.** Use this section to identify the target usernames, Active Directory groups, SharePoint Groups or email address of the account (source) you wish to delete permissions. You can use either:
 - The **Browse**  icon to select the username/groups, or
 - In the people picker text box, type usernames, Active Directory groups or email address separated by a semi colon (;), and then click the **Check Names**  icon to verify that you have typed valid usernames.

Delete Permissions From

You can enter usernames, domain group names, e-mail addresses or SharePoint group names. Separate them with semicolons.

Choose Users or Domain Groups

Zoe; DP\g_sales




Choose SharePoint Groups

Designers

- **Job Processing.** Select one of the [transaction types](#): **Run Now**, **Run Later** or **Both**. This option determines when the job will be processed. The default setting is **Both**.

Job Processing

Select when this job will be performed.

☒ Run Now 
☐ Run Later 
☐ Both 

- **Options.** Select or deselect the check box, **Alerts**. According to the permissions of the current user, alerts can be chosen to be included or not. For more information, see [Security Trimming](#).

4. Click **Next** to display the confirmation screen in the results pane.

Use this page to confirm delete permissions job.

Verify "Delete From" members

These members' permissions will be deleted.

DP\zoe
DP\g_sales
Designers

Note: Requested changes will be made only to sites, folders, lists, and list items where you are able to manage SharePoint permissions. If you are not able to manage permissions for a specific site, folder, list, or list item, changes will not be applied to that object.

OK

Cancel

5. Review the page. If you need to make changes, click the **Cancel**, otherwise click **OK**.
The *Delete Permissions* page is displayed stating that the DeliverPoint jobs have been successfully created. This page does not mean that the *Delete Permissions* DeliverPoint command is complete. The *Delete Permissions* command will not be processed until the DeliverPoint job is completed. DeliverPoint executes the job according to the timing of the [Transaction Type](#) selected.
6. Click **Return** to display the *Delete Permissions* screen, or click **Job Status** to display the [DeliverPoint Job Status and History](#) page, which you can use to monitor when the Copy Permissions DeliverPoint job.



Note: You can display the [DeliverPoint Job Status and History](#) page from the **View** Ribbon tab on the [DeliverPoint dashboard](#).

References

[<< Transfer Permissions](#)

[Revoke Permissions >>](#)

Revoke Permissions

“Revoke an accounts permissions”

Revoke Permissions is different to Delete Permissions. Delete Permissions will delete all permissions assigned to a specific account. Revoke Permissions allows you to remove a permission level from a user. Revoke Permissions is useful when duplicate permissions are assigned to an account such as Contribute and Edit. The Edit Permission Level could be revoked leaving just Contribute.

To use the **Revoke Permissions** command, complete the below method.

1. Navigate to the [DeliverPoint dashboard](#) and using the drop down on the **Grant Permissions** Ribbon button,
2. Select the scope using the Tree View for the operation.
3. Click the drop down on ‘Grant Permissions’ and select the ‘**Revoke Permissions**’ button.
4. Choose when you want the operation to run. Now, Later or Both.
5. Click Next and then Finish.

Revoke Permissions will either remove the user for a group, or remove a permission level if the permission level is directly assigned.

The screenshot displays the Lightning Tools application interface. At the top, a ribbon contains various icons for file and list management. The 'Grant Permissions' icon is selected, and a dropdown menu is open, showing the 'Revoke Permissions' option. Below the ribbon, the main area is titled 'Operation: Revoke Permissions' and contains instructions on how to configure a revoke permissions job. It includes fields for 'Revoke Permissions From' (with a hint to enter usernames, domain group names, etc.) and 'Choose Users or Domain Groups' (with a text input field). There is also a 'Choose SharePoint Groups' section with a list box. On the left side, a sidebar shows 'Permissions' and 'Select permissions to be revoked'. On the right side, a 'Revoke:' section contains checkboxes for 'Approve', 'Bretts Custom Permissions Level', 'Contribute', and 'Contribute without delete'.

Operation: Revoke Permissions
Revoke permissions from specific account

Use this page to configure a revoke permissions job for selected scope.

Revoke Permissions From
You can enter a usernames, domain group names, e-mail addresses or SharePoint group names.

Choose Users or Domain Groups
Enter names or email addresses...

Choose SharePoint Groups

Permissions
Select permissions to be revoked

Revoke:

- ☐ Approve
- ☐ Bretts Custom Permissions Level
- ☐ Contribute
- ☐ Contribute without delete

References

[<< Delete Permissions](#)

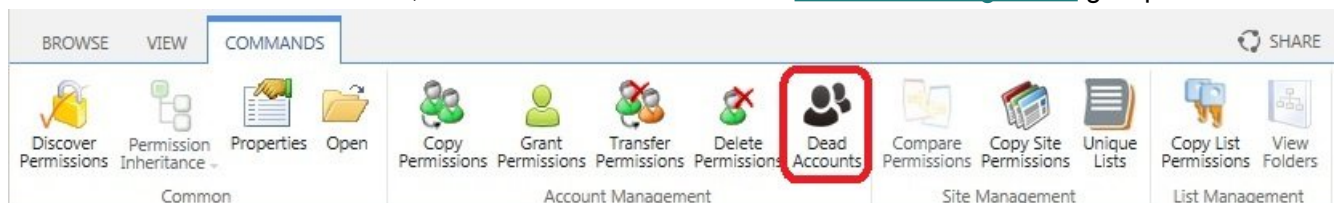
[Dead Account Detection >>](#)

Dead Account Detection

Dead Account Detection (DAD) displays all accounts found within Microsoft® SharePoint® that do not exist within Active Directory (AD) within the chosen scope in the treeview.

To use the **Dead Account Detection** command, complete the following steps:

1. Navigate to the [DeliverPoint dashboard](#) and using the **View** Ribbon tab, select either the [Farm Centric](#) or [Account Centric](#).
2. In the tree view, select those nodes, also known as SharePoint objects, to be included in the scope, for example, one or more site collections. You can only use the Dead Account commands when you select Server Farm, Web Applications, managed paths or site collections. It can not be used with other SharePoint objects, such as, sites or an accounts. The properties of the node selected are displayed in the dashboard's **Properties** pane.
3. On the **Commands** Ribbon tab, click **Dead Accounts** in the [Account Management](#) group.




The **Dead Account Detection** page is displayed in the dashboard results pane. The nodes included in the scope are displayed to the right of the page title.

A report is displayed in the results pane of the [DeliverPoint dashboard](#). When a user does not exist in AD, then a line is displayed for each site collection where the user has access, so you may see the same account multiple times in multiple site collections.

Operation: Dead Account Detection | Scope: Server Farm

Actions ▾

The following accounts were found in SharePoint but were not found in the authentication store (or disabled).

 Account	Disabled	Name	Email	Group	Site Auditor	Site Admin	Site Collection
<input type="checkbox"/> TRAINSBYDAVE\karla	False	Karla	Karla@trainsbydave.com	False	False	False	http://intranet/divisions/LT

Note Disabled or locked accounts do not appear in the report.

4. Using the **Report** Ribbon tab either:

- Click **Export to Spreadsheet**.

A **File Download** dialog box opens, click **Open** to open the report in Microsoft® Excel, or click **Save** to save the xls file. The xls file name is of the format, *Dead_Accounts_yyyymmdd.xls*.

- Select the check box to the left of one or more users, and then on the **Report** Ribbon tab, click **Delete Accounts**.

The *Operation: Delete Accounts* page is displayed in the results pane.

- Verify the information and then click **OK**.

The *Operation* screen is displayed stating that the DeliverPoint jobs have been created.

This page does not mean that the *Delete Accounts* DeliverPoint command is complete – this page is a confirmation that a DeliverPoint [Run Now](#) job has been created. The *Delete Accounts* command will not be processed until the DeliverPoint job is completed.

DeliverPoint executes the job according to the timing of the [Transaction Type](#) selected.

- Click **Job Status** to display the [DeliverPoint Job Status and History](#) page, which you can use to monitor the Delete Account DeliverPoint job.



Note: You can display the [DeliverPoint Job Status and History](#) page from the **View** Ribbon tab on the [DeliverPoint dashboard](#).

References


[<< Revoke Permissions](#)

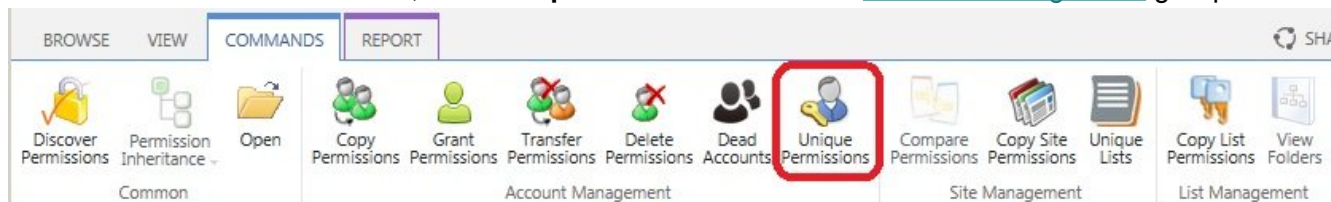
[Unique Permissions >>](#)

Unique Permissions

'View the account's unique permissions.'

To use the **Unique Permissions** command, complete the following steps:

1. Navigate to the [DeliverPoint dashboard](#) and using the **View** Ribbon tab, click [Account Centric](#).
2. In the search box, type one or more characters of a username and then click the  white arrow with a green background icon.
3. In the tree view, select the username to be included in the scope, or click the plus sign (+) and select a SharePoint object, such as a Web Application.
4. On the **Commands** Ribbon tab, click **Unique Permissions** in the [Account Management](#) group.












The *Operations: Unique Permissions* page is displayed in the results pane of the [DeliverPoint dashboard](#).


Operation: Unique Permissions for TRAINSBYDAVE\peter | **Scope: Server Farm**

Actions ▾


Account Memberships

Account	Defining Site Collection	Member Account
 TRAINSBYDAVE\peter		
 NT AUTHORITY\authenticated users		
 TRAINSBYDAVE\domain users		
 Style Resource Readers	http://intranet	NT AUTHORITY\authenticated users
 TrainsbyDave Intranet Visitors	http://intranet	NT AUTHORITY\authenticated users
 TrainsbyDave Intranet Owners	http://intranet	TRAINSBYDAVE\domain users
 Finance Owners	http://intranet/divisions/financials	TRAINSBYDAVE\domain users
 LT Owners	http://intranet/divisions/LT	TRAINSBYDAVE\peter
 Sales Owners	http://intranet/divisions/sales	TRAINSBYDAVE\domain users

Site Collection Administrator Designations

Account	Site Collection
 TRAINSBYDAVE\peter	http://intranet/divisions/LT

Unique Site Permissions

Account	Site Collection	Site	Permission Level
 Peter P. Coventry	http://intranet/divisions/LT	http://intranet/divisions/LT	Full Control

The report displays information in the following sections:

- **Account Membership.** The Account, Defining Site Collection and Member Account.
- **Site Collection Administration Designations.** Account and Site Collection.
- **Unique Site Permissions.** The Account, Site Collection, Site and Permission Level.
- **Unique List Permissions.** The Account, Site Collection, Site, List Name, and Permission Level.

Note The account, site collection, site, list name and permission level are all hyperlinks, and when clicked open the respective page that details more information about the SharePoint object, for example, by clicking on the site collection, the Permissions page for that site collection is displayed in a separate browser window.

You can save the report. In the results pane, use the **Report** Ribbon tab and click **Export to Spreadsheet**. The Microsoft® Excel spreadsheet file name is of the format, *Unique_Permissions_yyyymmdd.xls*.

References

[<< Dead Account Detection](#)

[Site Management >>](#)

Site Management

[DeliverPoint 2013](#) allows you to manage SharePoint permissions in Microsoft® SharePoint® Server 2013 or Microsoft® SharePoint Foundation 2013 on-premises deployments. From the tree view on the [DeliverPoint dashboard](#) by clicking a SharePoint object you can initiate DeliverPoint commands, from the **Commands** Ribbon tab. The commands in the **Site Management** group are listed below.



Note, not all commands can be completed on all SharePoint objects.

- [Compare Site Permissions.](#)
- [Copy Site Permissions.](#)
- [Unique Lists](#)

Other DeliverPoint commands that you may wish to complete at a site level are also found on the **Commands** Ribbon tab, include:

- [Discover Site Permissions.](#)
- [Inherit or break Permission Inheritance.](#)
- [Properties](#)
- **Open** site in new browser window / tab.
- [Copy List Permissions.](#)

References

- [← DeliverPoint dashboard](#)
- [← Account Management](#)
- [← Site Management](#)
- [List Management →](#)

Compare Site Permissions

“Generates permissions comparison report for selected sites.”

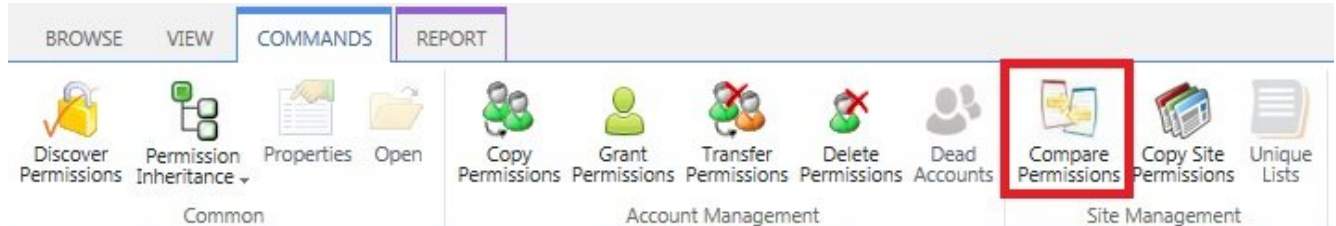
✿ This DeliverPoint action can only be used to compare sites.

To use the **Compare Site Permissions** action, complete the following steps:

1. Navigate to the [DeliverPoint dashboard](#) and on the **View** Ribbon tab, click either the [Farm Centric](#) or [Account Centric](#).
2. In the tree view, select one or more sites, to be included in the scope. This action can not be completed on an accounts. A summary of the properties of the nodes selected are displayed in the dashboard's *Properties* pane.

Note: Child nodes are not automatically included.

3. On the **Commands** Ribbon tab, click **Compare Permissions** in the [Site Management](#) group.



Note If you only select one site, then the *Compare Permissions* command is inactive, you must select at least 2 sites where you have the *Enumerate Permissions* rights before this command is available to you on the Ribbon.

The *Operation: Web permissions comparison report* page is displayed in the dashboard results pane. The nodes included in the scope are display to the right of the page title.

Operation: Web permissions comparison report. Scope: **Demos, BCS Demo, Asset Tracking**

DP\speakers	Edit Limited Access	Limited Access AllowCreateEXT	Edit Limited Access
DP\students	Read	Read	Read
DP\teachers	Edit Limited Access	Limited Access AllowCreateEXT	Edit Limited Access
dp\julia	Full Control	Full Control	Full Control
dp\matt	.	Design	.
dp\michael	.	.	.
NT AUTHORITY\LOCAL SERVICE	.	.	.
dp\phill	.	.	.
dp\poppy	Edit Limited Access	Limited Access AllowCreateEXT	Edit Limited Access
dp\rrio	Full Control	Full Control	Full Control
dp\sara	Full Control Limited Access	Full Control Limited Access	Full Control Limited Access

Last Interrogation: 12 NOV at 02:1

- To export the report, on the Report Ribbon tab, click **Export to Spreadsheet** in the **Actions** group.
The Microsoft® Excel spreadsheet file name is of the format,
Compare_Web_Permissions_yyyymmdd.xls.

References

[<< Site Management](#)

[Copy Site Permissions >>](#)

Copy Site Permissions

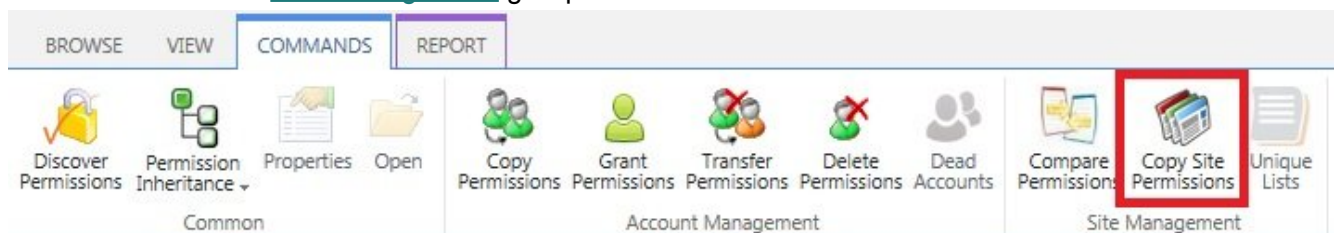
“Copy source site permissions to target sites”

DeliverPoint allows you to “copy” the permission settings of a site (site1) to other sites (site2, site3, etc.). DeliverPoint uses the following rules during the copy operation:

1. Sites with inherited permissions will be ignored.
2. Sites where a user does not have the *Manage Permissions* rights will be ignored.
3. If a user tries to use the *Copy Site Permissions* command, and they have no *Enumerate Permissions* rights over the source site, the DeliverPoint operation will have no affect.
4. If the target site inherits its permission levels from the parent site, any missing permission levels will be ignored. For example, if *site1* has a custom permission level named *PermLevel/Special*, and *site2* does not that same permission level, and inherits permission levels from its parent site, then, all users/groups from *site1* who have some assignment of permissions through *PermLevel/Special* will be copied without that assignment.

To use the **Copy Site Permissions** command, complete the following steps:

1. Navigate to the [DeliverPoint dashboard](#) and then on the **View** Ribbon tab, click either the [Farm Centric](#) or [Account Centric](#).
2. In the tree view, select any node, and then on the **Commands** Ribbon tab, click **Copy Site Permissions** in the [Site Management](#) group.



The *Operation: Copy Web Permissions – Selecting source and target webs* page is displayed in the dashboard results pane.

Operation: Copy Web Permissions - Selecting source and target webs

Use this page to specify source and target webs. Select source web from first tree control and then select target webs from second tree control. Not accessible web nodes are disabled.

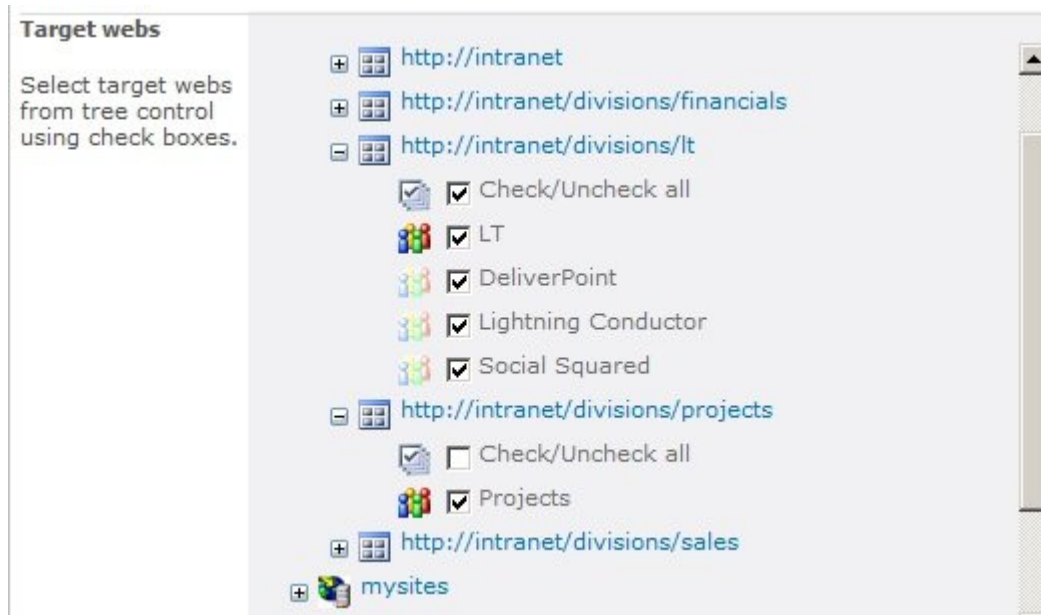
Source Web

Select the source web from tree control using check boxes.

- ☐ intranet
- ☐ mysites
- ☐ projecthome
- ☐ tbd-records
- ☐ trainsbydave content type hub
- ☐ wea training

Complete the information in the following five sections – you may need to scroll down to see these sections and the *Next* button:

- **Source Web:** Click the plus sign (+) to expand the appropriate Web Application, continue to expand SharePoint objects until you find the site you wish to use as the source site, and then select the checkbox to the right of the site. You can only select one site as the source site.
- **Target Web:** Expand the SharePoint object in the target tree view. Select the check boxes for those site you wish to copy the source site permissions. You will see a check box above the top level site of each site collection, labelled, **Check/Uncheck all**, that allows you to select or clear the check boxes for all sites in the site collection.



- **Job Processing:** Select one of the [transaction types](#): **Run Now**, **Run Later** or **Both**. This option determines when the job will be processed. The default setting is **Both**.

Job Processing

Select when this job will be performed.

- ☒ Run Now [?](#)
☐ Run Later [?](#)
☐ Both [?](#)

- **Clone Options:**
 - Clear or select the **Clone groups in target web** checkbox, if you want to have missing group assignments, including their member accounts, to be created in the target site's site collection. For example, when you select the checkbox, and *Group1* is assigned permissions in *site1* and *site2* does not contain *Group1*, the DeliverPoint action will create a new group with the same name in the *site2* and will assign to that group the required permissions.
 - Select **Clone role definitions in target web** checkbox, if you want to copy the permission level settings from the target site to the source site. By default the permission levels used by the source site are not copied to the target site.

- Click **Next** to display the confirmation screen in the results pane.

Operation: Copy Web Permissions- Verifying source and target webs

Use this page to confirm the copy web permissions job.

Verify source web	
This web's permissions will be copied.	http://intranet/divisions/financials
Verify target webs	
The copied permissions will be appended to these webs.	http://intranet/divisions/lt http://intranet/divisions/lt/dp http://intranet/divisions/lt/lcwp http://intranet/divisions/lt/ss http://intranet/divisions/projects

Note: Requested changes will be made only to sites where you are able to manage SharePoint permissions. If you are not able to manage permissions for a specific site changes will not be applied to that object.

OK Cancel

- Review and then click **OK**.

The *Operation completed successfully* screen is displayed in the results pane. This page does not mean that the Copy Site Permissions DeliverPoint action is complete – this page is a confirmation that DeliverPoint job(s) have been created. DeliverPoint will create one *Clone Web Permissions* job for each target site. If you choose the transaction type: *Both*, then two DeliverPoint jobs will be created for each target site. The Copy Site Permissions action will not be processed until the DeliverPoint job(s) are completed. DeliverPoint executes the job according to the timing of the [Transaction Type](#) selected.

Operation: Copy Permissions | Scope: Demos, Products

Jobs have been successfully created to copy the selected member's permissions.

[Return](#) | [Job Status](#)

- Click **Return** to display the *Operation: Copy Web Permissions* screen so you can complete another *Copy Site Permissions*, or click **Job Status** to display the [DeliverPoint Job Status and History](#) page, which you can use to monitor the *Clone Web Permissions* job(s).



Note: You can display the [DeliverPoint Job Status and History](#) page from the **View** menu on the [DeliverPoint dashboard](#).

References

[<< Compare Site Permissions](#)





[Unique Lists Detection >>](#)

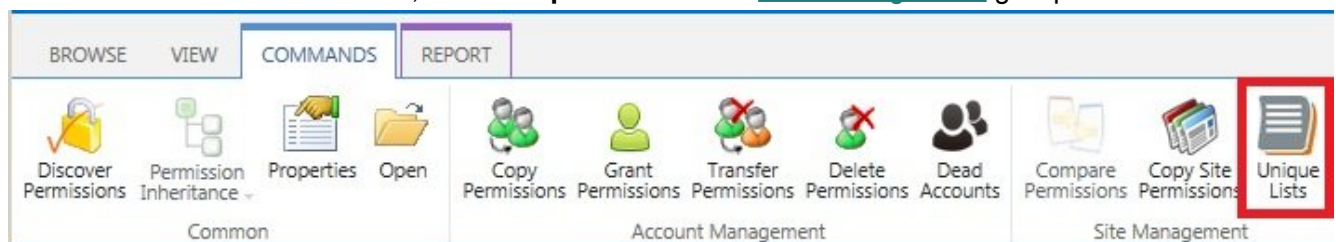
Unique Lists Detection

'Discover Lists with unique permissions'.

The *Unique Lists Detection* action displays all lists within the selected scope that have unique permissions (not inherited from owner site). Allowed scope nodes are – Farm, Web Application and Site Collections. By default [permission inheritance](#) cascades down from the top-level site in a site collection to sub sites, lists, libraries, list items and files. This action is useful in identifying where permission inheritance was stopped and different permissions assigned to lists and libraries. See the whitepaper, [Best practices for using fine-grained permissions](#).

To use the **Unique Lists** DeliverPoint action, complete the following steps:

1. Navigate to the [DeliverPoint dashboard](#), on the **View** Ribbon tab, click either the [Farm Centric](#) or [Account Centric](#).
2. In the tree view, select those nodes, also known as SharePoint objects, to be included in the scope, for example, one or more site collections. This command can be completed on the farm , Web Application , Managed Path  or site collections .
3. On the **Commands** Ribbon tab, click **Unique Lists** in the [Site Management](#) group.



The *Operation: Lists with Unique Permissions* page is displayed in the dashboard results pane. The nodes included in the scope are display to the right of the page title.

Server Farm

intranet.dp.local

(root)

personal

sites

SharePoint - 80

Teams

Operation: Lists with Unique Permissions. Scope: sites

Site Collection	Site	List Title
http://intranet.dp.local/sites/Teams	http://intranet.dp.local/sites/Teams	TaxonomyHiddenList
http://intranet.dp.local/sites/LT	http://intranet.dp.local/sites/LT	Translation Packages
http://intranet.dp.local/sites/LT	http://intranet.dp.local/sites/LT	Relationships List
http://intranet.dp.local/sites/LT	http://intranet.dp.local/sites/LT	Style Library
http://intranet.dp.local/sites/LT	http://intranet.dp.local/sites/LT	Master Page Gallery
http://intranet.dp.local/sites/LT	http://intranet.dp.local/sites/LT	Site Collection Images
http://intranet.dp.local/sites/LT	http://intranet.dp.local/sites/LT	Variation Labels
http://intranet.dp.local/sites/LT	http://intranet.dp.local/sites/LT	Quick Deploy Items
http://intranet.dp.local/sites/LT	http://intranet.dp.local/sites/LT	Suggested Content Browser Locations
http://intranet.dp.local/sites/LT	http://intranet.dp.local/sites/LT	Translation Status
http://intranet.dp.local/sites/LT	http://intranet.dp.local/sites/LT	Device Channels
http://intranet.dp.local/sites/LT	http://intranet.dp.local/sites/LT	Cache Profiles

Last Interrogation: 12 NOV at 02:16AM

sites

Managed Path

Site Collections:8

All links on the report open new browser windows. The links for the Site Collection and Site open the home pages for the site. The link for the list, open the default view for the list.

- To export the report, on the **Report** Ribbon tab, click **Export to Spreadsheet** in the **Actions** group. The Microsoft® Excel spreadsheet file name is of the format, *Unique_Lists_yyyymmdd.xls*.

References

[Best practices for using fine-grained permissions](#)

[<< Copy Site Permissions](#)

[List Management >>](#)

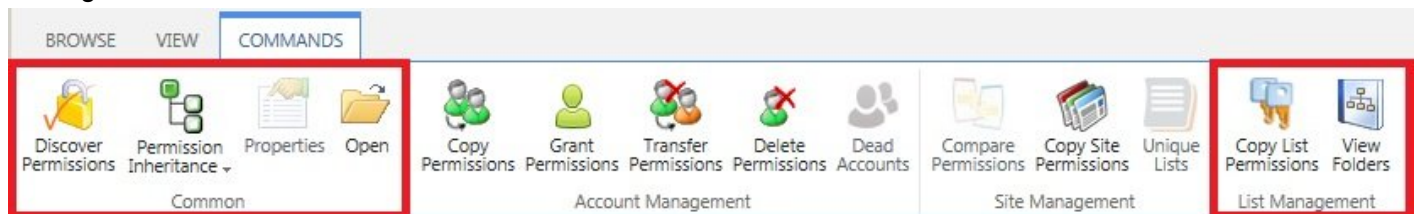
Page 158 of 268

List Management

You can use DeliverPoint list management commands from either the DeliverPoint dashboard, when the **Show Lists and Libraries In Report** check box is selected on the [DeliverPoint Configuration](#) page, or from the DeliverPoint Ribbon tab, when you are displaying the list or library in the browser. You can also add a column a list / library, based on the [DeliverPoint inheritance field](#) to display folder, list item, file permission inheritance in views.

Using list management from the DeliverPoint dashboard

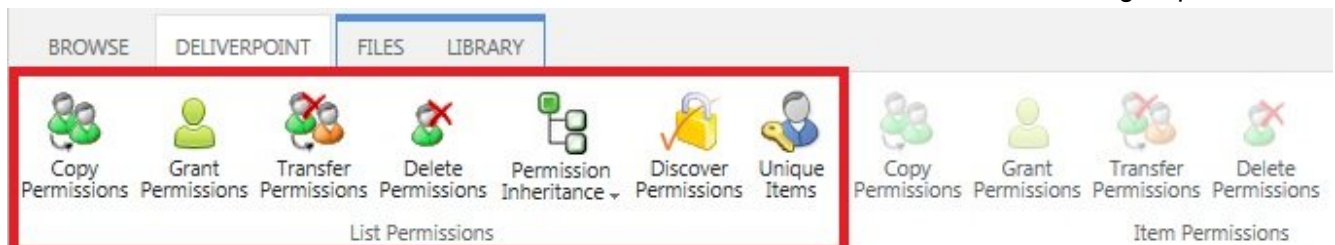
On [DeliverPoint dashboard](#) in either the [Farm Centric](#) or [Account Centric](#) view can select the following list management actions on the **Commands** Ribbon tab:



- In the **Common** group:
 - [Discover Permissions](#)
 - [Permission Inheritance](#)
 - **Open** to open the list or library in a new browser windows / tab.
- In the **List Management** group:
 - [Copy List Permissions](#)
 - **View Folders** to display the folders in a list or library.

Using list Management from the DeliverPoint Ribbon tab

1. Navigate to the list or library where you want to use the DeliverPoint list permissions commands.
2. On the **DeliverPoint** Ribbon tab, click a list-level commands in the **List Permissions** group.



These list-level commands are:

- [Copy Permissions](#)
- [Grant Permissions](#)
- [Transfer Permissions](#)
- [Delete Permissions](#)
- [Permission Inheritance](#)
- [Discover Permissions](#)
- [Unique Items](#)

References

[<< Unique Lists Detection](#)

[Copy List Permissions >>](#)

Copy List Permissions

“Copy source list permissions to target lists”

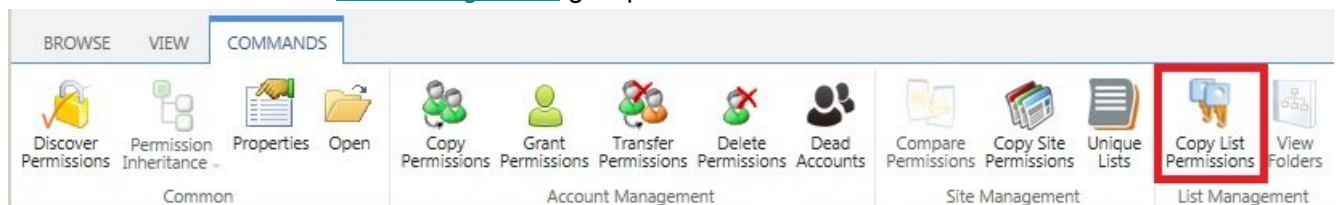
DeliverPoint provides an interface to copy the list permissions (list1) to other lists (list2, list3, etc.).

DeliverPoint uses the following rules during the copy:

1. Lists with inherited permissions will be ignored.
2. Lists where user does not have the *Manage Permissions* rights will be ignored.
3. If a user tries to use the *Copy Lists Permissions* command, and they have no *Enumerate Permissions* rights over the source list, the DeliverPoint operation will have no affect.
4. When the target list's parent site has any missing permission levels, all assignments that use those missing permission levels will be ignored. For example, when *user1* is mapped to both the Read and *PermLevel/Special* permission levels for the source list in *site1*, and *site2* has Read but no *PermLevel/Special* permission level, then, *user1* will be copied without *PermLevel/Special*, and *user1* is mapped to only the *Read* permission level for the *list2*.

To use the **Copy List Permissions** command, complete the following steps:

1. Navigate to the [DeliverPoint dashboard](#), on the **View** Ribbon tab, click either the [Farm Centric](#) or [Account Centric](#).
2. In the tree view:
Either select any site or site collection, and then on the **Commands** Ribbon tab, click **Copy List Permissions** click in the [List Management](#) group.



or, if lists and libraries are displayed in the tree view, select a list or library, and then on the **Commands** Ribbon tab, click **Copy List Permissions** click in the [List Management](#) group.

The *Operation: Copy List Permissions* page is displayed in the dashboard results pane.

3. Complete the information in the following five sections:

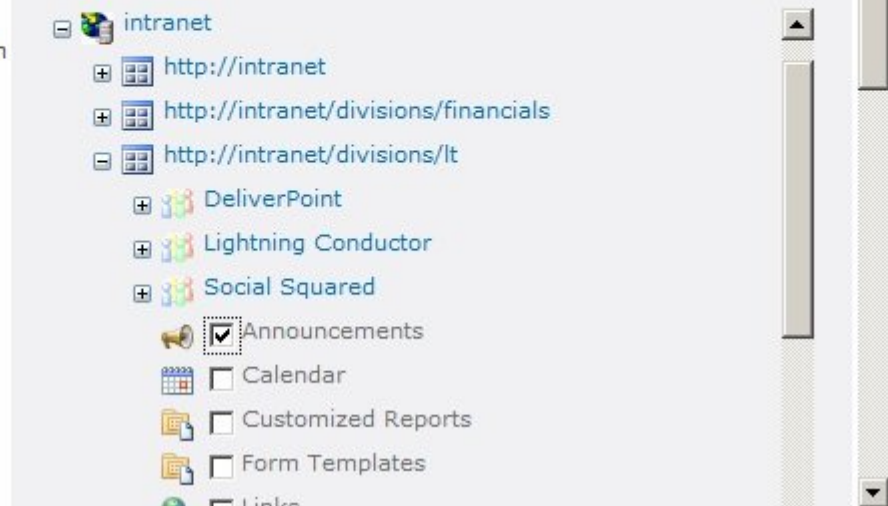
- **Source List:** Click the plus sign (+) to expand the appropriate Web Application, continue to expand SharePoint objects until you find the list you wish to use as the source list, and then select the checkbox to the right of the list. You can only select one list as the source list.

Operation: Copy List Permissions - Selecting source and target lists

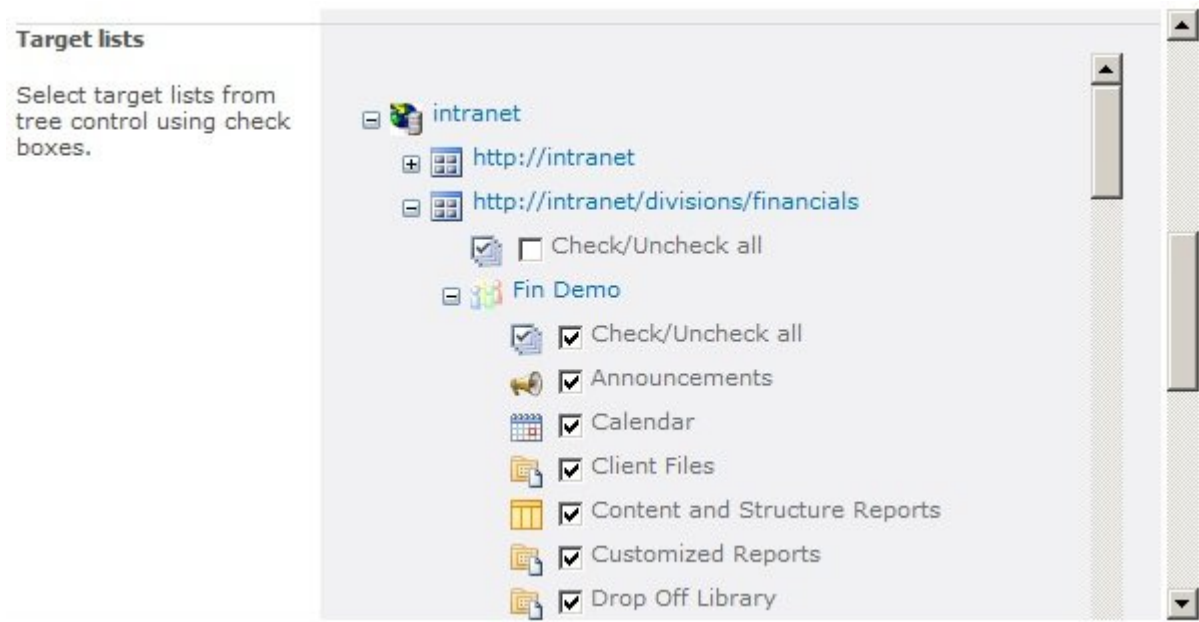
Use this page to specify source and target lists. Select source list from first tree control and then select target lists from second tree control. Not accessible web and list nodes are disabled.

Source List

Select the source list from tree control using check boxes.



- **Target lists:** Expand the SharePoint object in the target tree view. Select the check boxes for those lists you wish to copy the source list permissions. You will see a check box above the top level site of each site collection and each site, labelled, **Check/Uncheck all**, that allows you to select or clear the check boxes for all lists in the site collection, or site.



- **Job Processing:** Select one of the [transaction types](#): **Run Now**, **Run Later** or **Both**. This option determines when the job will be processed. The default setting is **Both**.

Job Processing

Select when this job will be performed.

- ☒ Run Now

☐ Run Later

☐ Both

- **Clone options:**
 - Clear or select the **Clone groups in target web** checkbox, if you want to have missing group assignments, including their member accounts, to be created in the target site's site collection. For example, when you select the checkbox, and *Group1* is assigned permissions in *site1* (the source list site) and *site2* (the target list site) does not contain *Group1*, the DeliverPoint action will create a new group with the same name in the *site2* and will assign to that group the required permissions for the target list.
 - Select **Clone role definitions in target web** checkbox, if you want to copy the permission level settings from the target list to the source list. By default the permission levels used by the source list are not copied to the target list.

Clone options Choose this option if you want to have missing group assignments be created in target web's site collection with their members.	Include: <input checked="" type="checkbox"/> Clone groups in target web
Options Select additional options.	Include: <input checked="" type="checkbox"/> Alerts

Next >

- **Options:** Select or deselect the check box, **Alerts**. According to the permissions of the current user, alerts can be chosen to be included or not. For more information, see [Security Trimming](#).

6. Click **Next** to display the confirmation screen in the results pane.

Operation: Copy List Permissions - Verifying source and target lists

Use this page to confirm the copy list permissions job.

Verify source list This list's permissions will be copied.	http://intranet/divisions/lt/lists/announcements/allitems.aspx
Verify target lists The copied permissions will be appended to these lists.	http://intranet/divisions/financials/demo/lists/announcements/allitems.aspx http://intranet/divisions/financials/demo/lists/calendar/calendar.aspx http://intranet/divisions/financials/demo/client files/forms/all documents.aspx http://intranet/divisions/financials/demo/reports list/allitems.aspx http://intranet/divisions/financials/demo/analyticsreports/forms/allitems.aspx http://intranet/divisions/financials/demo/dropofflibrary/forms/allitems.aspx http://intranet/divisions/financials/demo/expenses/forms/allitems.aspx http://intranet/divisions/financials/demo/formservertemplates/forms/all forms.aspx http://intranet/divisions/financials/demo/lists/links/allitems.aspx http://intranet/divisions/financials/demo/lists/product sales/allitems.aspx http://intranet/divisions/financials/demo/project documents/forms/allitems.aspx http://intranet/divisions/financials/demo/reusablecontent/content preview.aspx http://intranet/divisions/financials/demo/salescontracts/forms/allitems.aspx

7. Review and then click **OK**. You may need to scroll down to see the **OK** button.

The *Operation completed successfully* screen is displayed in the results pane. This page does not mean that the Copy List Permissions DeliverPoint action is complete – this page is a confirmation that DeliverPoint job(s) have been created. DeliverPoint will create one *Clone List Permissions* job for

each target list. If you choose the transaction type: *Both*, then two DeliverPoint jobs will be created for each target list. The Copy List Permissions action will not be processed until the DeliverPoint job(s) are completed. DeliverPoint executes the job according to the timing of the [Transaction Type](#) selected.

Operation: Copy Permissions | Scope: Demos, Products

Jobs have been successfully created to copy the selected member's permissions.

[Return](#) | [Job Status](#)

8. Click **Return** to display the *Operation: Copy List Permissions* screen so you can complete another *Copy List Permissions* action, or click **Job Status** to display the [DeliverPoint Job Status and History](#) page, which you can use to monitor the *Clone List Permissions* job(s).

 **Note:** You can display the [DeliverPoint Job Status and History](#) page from the **View** menu on the [DeliverPoint dashboard](#).

References

[<< List Management](#)

[Unique List Items Detection >>](#)

Unique List Items Detection

The Unique List Items Detection action, displays all list items for specified list that have unique permissions, that is, permissions not inherited from parent list.

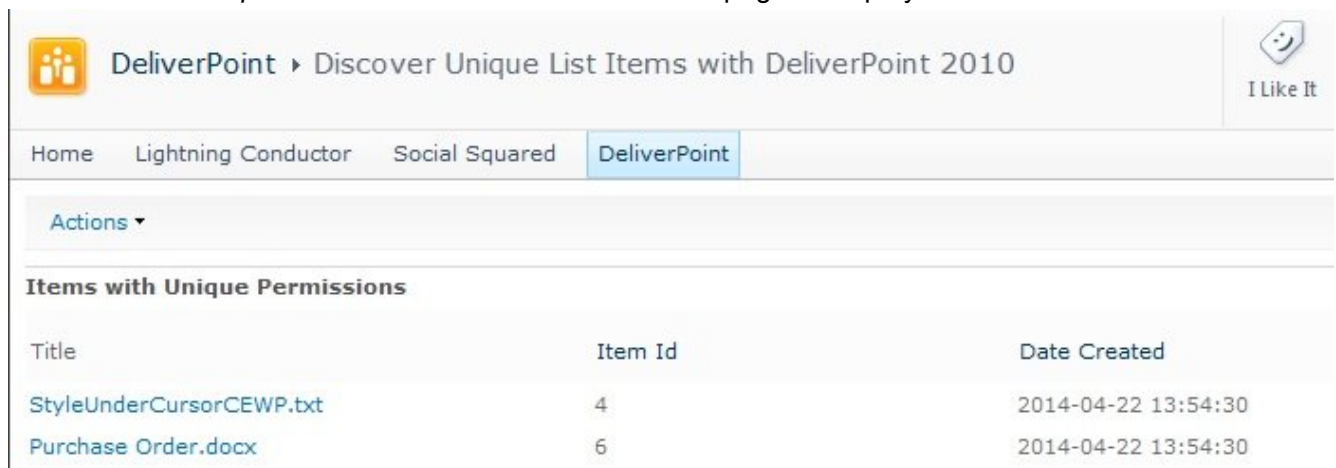
By default [permission inheritance](#) cascades down from the top-level site in a site collection to sub sites, lists, libraries, list items and files. In SharePoint, there is a maximum number of unique security scopes that can be used for a list or a library, in SharePoint 2013, this number, known as [security scope threshold](#), is 50,000. Although Microsoft recommends keeping the number of unique security scopes per list lower than this number.

Creating unique permissions on folder, list items and files can affect SharePoint performance. You may find that you are more likely to be affected by this, when users have created workflows that break inheritance at the item level. Therefore using this DeliverPoint action is useful in identifying where permission inheritance was stopped and different permissions assigned to list items and files. See [Best practices for using fine-grained permissions](#).

To use the **Unique Items** action, complete the following steps:

1. Navigate to the list / library where you want to use the DeliverPoint action.
2. On the **DeliverPoint** Ribbon tab, click **Unique Items** in the **List Permissions** group.

The *Discover Unique List Items with DeliverPoint 2013* page is displayed.



Title	Item Id	Date Created
StyleUnderCursorCEWP.txt	4	2014-04-22 13:54:30
Purchase Order.docx	6	2014-04-22 13:54:30

Under the **Title** column, click the item link to display the properties of the item, where you can

manage the permissions of the item.

3. To export the report, click the **Actions** menu, and then click **Export to Spreadsheet**. The Microsoft® Excel spreadsheet file name is of the format, *Unique_Items_yyyymmdd.xls*.

References

[Best practices for using fine-grained permissions](#)

[<< Copy List Permissions](#)

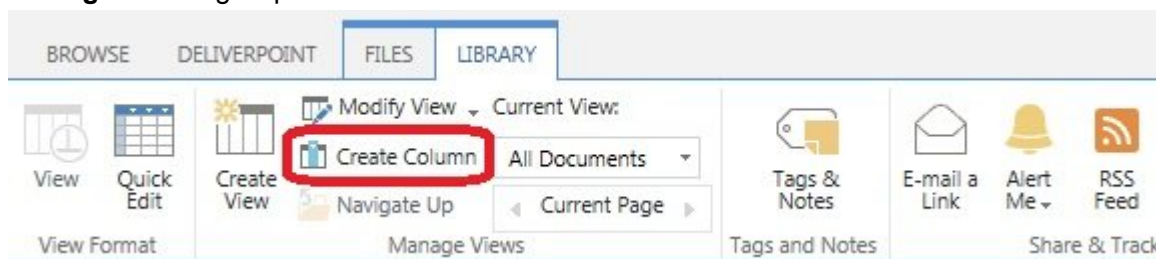
[DeliverPoint Inheritance Field >>](#)

DeliverPoint Inheritance Field

Within any list or library Field type you can add the DeliverPoint Inheritance Field. This is a custom column which when added to a view displays a permissions inherited/broken inheritance indicator which acts as a hyperlink to the [Discover Permissions](#) page for that item/folder.

To add the DeliverPoint Inheritance Field to a list or library, complete the following steps:

1. Navigate to the list or library, and then on the **List / Library** Ribbon tab, click **Create Column** in the **Manage Views** group.



2. On the *Create Column* dialog, type a name for the list in the **Column name** text box, for example, **Permission Inheritance** and then select **DeliverPoint inheritance field**.

Create Column

Name and Type
Type a name for this column, and select the type of information you want to store in the column.

Column name:

The type of information in this column is:

- ☐ Single line of text
- ☐ Multiple lines of text
- ☐ Choice (menu to choose from)
- ☐ Number (1, 1.0, 100)
- ☐ Currency (\$, ¥, €)
- ☐ Date and Time
- ☐ Lookup (information already on this site)
- ☐ Yes/No (check box)
- ☐ Person or Group
- ☐ Hyperlink or Picture
- ☐ Calculated (calculation based on other columns)
- ☐ External Data
- ☒ **DeliverPoint inheritance field**
- ☐ Managed Metadata




Earlier versions of client programs might not support this type of column. Adding this column might block those programs from saving documents to this library.

Additional Column Settings


3. If the view that was displayed was not the default view then a check box is displayed, **Add to default view**. Select if you want the DeliverPoint inheritance column added to the default view.

4. Scroll to the bottom of the page, and then click **OK**.

The *DeliverPoint Inheritance* column is created. If you used the above steps when the default view is displayed the column is automatically added to the default view.

✓	Name	Modified	Modified By	Permission inheritance
	DP Folder 1	... October 03	<input type="checkbox"/> Brett	
	DP Folder 2	... October 03	<input type="checkbox"/> Brett	
	SPS2014_Speaker_Submission	... November 13	<input type="checkbox"/> Brett	

When the folders / items where permission is inherited – the inheritance icon  is greyed. When

permission inheritance is broken, then the inheritance icon  is not transparent.

Note To find more information on the permissions for the list / folder / item / file, use the [Discover Permissions](#) command. To add the column based on the DeliverPoint inheritance field to other views, see the procedures below.

* The image file, **UniquePermissions.png**, used in the DeliverPoint inheritance field is stored the **../images/DeliverPoint/Fields** folder in the **15** hive of each front-end server in your Microsoft SharePoint farm. Your organization could replace this file with their own image if they prefer.

To remove the DeliverPoint inheritance column from a list or library, complete the following steps:

1. Navigate to the list / library where you want to remove the column based on the *DeliverPoint inheritance field* that you created previously.
2. On the **List / Library** Ribbon tab, click **List / Library Settings** to display the *Settings* page.
3. In the **Columns** section, click on the name of the DeliverPoint inheritance field column to display the *Edit Column* page.
4. At the bottom of the page, click **Delete**.
5. A Message from webpage dialog box is displayed, click **OK** to confirm the removal of the column.

To add the DeliverPoint Inheritance column to a view, complete the following steps:

1. Navigate to the list / library where you previously created a column based on the *DeliverPoint inheritance field*.
2. On the **List / Library** Ribbon tab, in the **Manage Views** group, change to the view where you want to add the DeliverPoint inheritance column.
3. On the List / Library Ribbon tab click **Modify View** in the **Manage Views** group to display the **Edit View** page.
4. Select the checkbox to the right of the column based on the DeliverPoint inheritance field.
5. Scroll to the bottom of the page, and click **OK**.

To remove the DeliverPoint Inheritance column from a view, complete the following steps:

1. Navigate to the list / library where you previously added to a view the column based on the *DeliverPoint inheritance field*.

2. On the **List / Library** Ribbon tab, in the **Manage Views** group, change to the view where you want to remove the DeliverPoint inheritance column.
3. On the List / Library Ribbon tab click **Modify View** in the **Manage Views** group to display the **Edit View** page.
4. Clear the checkbox to the right of the column based on the DeliverPoint inheritance field.
5. Scroll to the bottom of the page, and click **OK**.

References

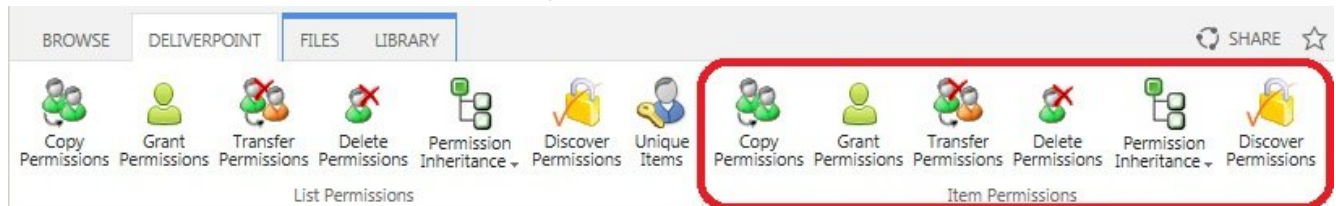
[<< Unique List Items Detection](#)

[Item Permissions >>](#)

Item Permissions

To use the Item Permissions commands on a folder, list item or file, complete the following steps:

1. Navigate to the list where you want to use the DeliverPoint item commands.
2. Click to the left of the folder, list item or file, and then on the **DeliverPoint** Ribbon tab, click an item-level command in the **Item Permissions** group.



These item level commands are:

- [Copy Permissions](#)
- [Grant Permissions](#)
- [Transfer Permissions](#)
- [Delete Permissions](#)
- [Permission Inheritance](#)
- [Discover Permissions](#)

[Troubleshooting >>](#)

[<< DeliverPoint Inheritance Field](#)

Troubleshooting

This section contains issues that may be experienced when installing or using DeliverPoint 2013:

- [Missing: DeliverPoint Timer Jobs](#)
- [Missing link: Manage LightningTools products licensing](#)

Missing: DeliverPoint Timer Jobs

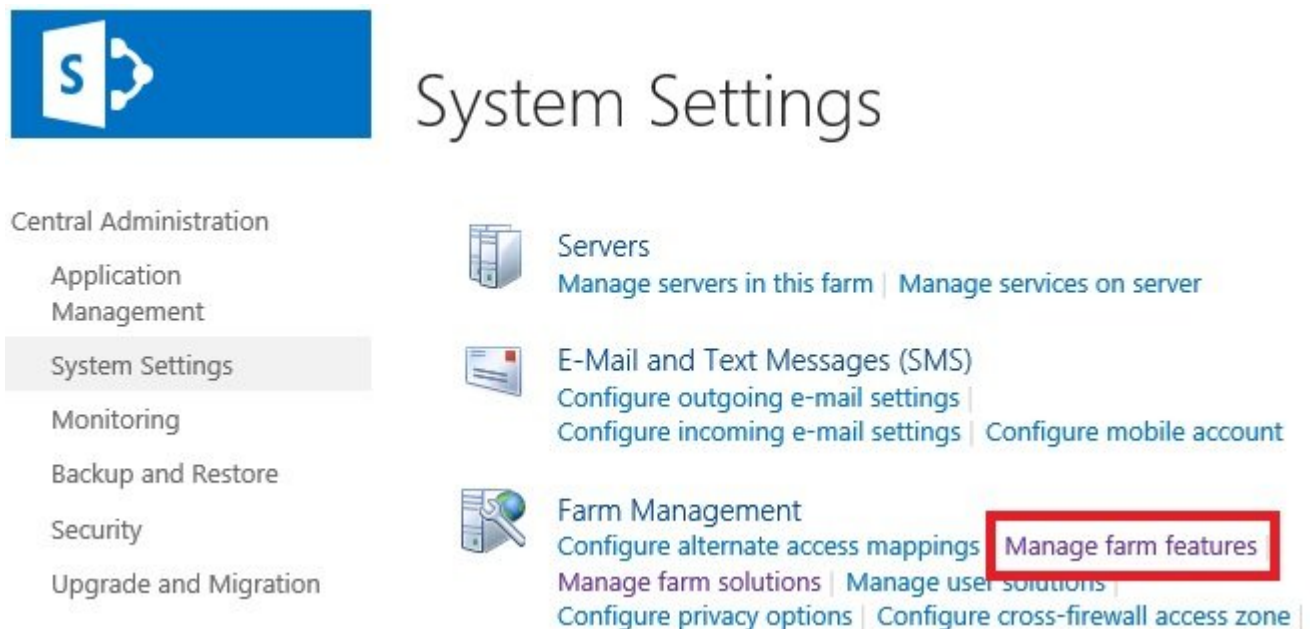
Symptom:

On the **Job Definition** page of the SharePoint 2013 Central Administration web site, the three LightningTools DeliverPoint timer jobs are missing.

Resolution:

Activate the LightningTools – DeliverPoint timerjobs farm feature using the following steps:

1. In the browser, on the Quick Launch of the Microsoft SharePoint Central Administration web site, click **System Settings**, and then under **Farm Management**, click **Manage farm features**.



2. On the **Manage Farm Features** page, to the right of **LightningTools – DeliverPoint 2013 TimerJobs**, click **Activate**.

Missing: Manage Lightning Tools Product Licensing link

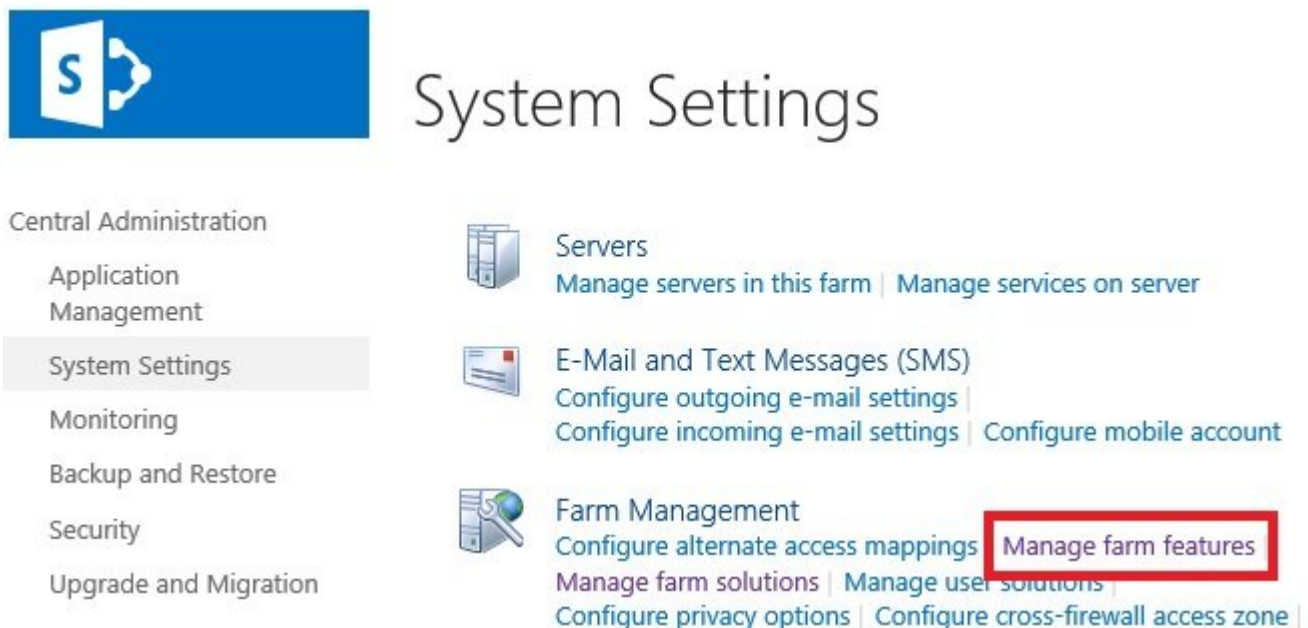
Symptom:

On the **System Settings** page of the SharePoint 2013 Central Administration web site, under **Farm Management**, the link – **Manage Lightning Tools products licencing** – is missing.

Resolution:

Activate the Manage Licensing Of DeliverPoint farm feature using the following steps:

1. In the browser, on the Quick Launch of the Microsoft SharePoint Central Administration web site, click **System Settings**, and then under **Farm Management**, click **Manage farm features**.



2. On the **Manage Farm Features** page, to the right of **Manage licensing of DeliverPoint** click **Activate**.

DeliverPoint SharePoint Online Add-In for Office 365

The DeliverPoint SharePoint Online Add-In for Office 365 allows users to find who has access to a given Microsoft® SharePoint® object within a site collection and how that access is given. The DeliverPoint [Discover Permissions](#) action is a real-time feature, that is, if an account is newly mapped to a permission level on a SharePoint object, such as a site, list, library, file, or item, the account will be found immediately in the [Discover Permissions report](#) for the object.



If you are new to managing permissions in SharePoint Online which comes with your [Office 365™](#) tenant, then you will find some useful links in the [References](#) section at the bottom of this page.

References

- [Introduction: Control user access with permissions](#)
- [Video: Understanding permissions in SharePoint](#)
- [Plan your permissions strategy](#)
- [Plan sites and manage users](#)
- [Plan your permissions strategy](#)
- [Governance: Permission Management](#)

- [Installation and Configuration of the DeliverPoint Add-In >>](#)
- [Using the DeliverPoint add-in →](#)

Installation and Configuration of the DeliverPoint Add-In

This section details how to install the DeliverPoint add-in from [Lightning Tools](#), so it can be used to report on permissions within SharePoint® Online. The installation of the DeliverPoint add-in is a four-step process:

- Install the add-in by getting the add-in from the Lightning tools and [uploading it into your organization's Office 365 app catalog](#).
- Create an [Azure application](#) with access to your Office 365 domain and obtaining a client-id and secret key of the Azure application.
- [Add the Add-In](#) to a SharePoint site.
- [Configure the Add-In](#) with the tenancy domain URL, and the Azure Add-In client-id and secret key.

[<< DeliverPoint SharePoint Online Add-In for Office 365](#)

[Upload Add-In to App Catalog >>](#)


Upload Add-In to App Catalog

This section details how to install the DeliverPoint add-in from [Lightning Tools](#), so it can be used on [Office 365™](#) sites. By completing the steps in this section, the DeliverPoint add-in appear on the Your Apps page, under Apps you can add, for all sites within an [Office 365™](#) tenant.

! To use the following method to install the DeliverPoint add-in to an Office 365 tenant, you must be an [Office 365 global admin](#).

1. Download the Add-In from: [Lightning Tools](#)
2. Navigate to your [SharePoint admin center](#).

Note: If you are unsure where your [SharePoint admin center](#) site is:

- a. Click the [Apps Launcher](#)  icon in the top left and then click **Admin** to display the [Office 365 admin center](#).
 - b. At the bottom of the Quick Launch, expand **Admin** and then click **SharePoint** to display the *SharePoint admin center*.
3. On the Quick Launch, click **apps**, and then click **App Catalog** to display the home page of the App Catalog site.
 4. On the Quick Launch, click **Apps for SharePoint**.
 5. Click **Upload** to display the **Add a document** dialog.
 6. Click **Browse** to open the **Choose File to Upload** dialog box.
 7. Navigate to where you have stored the DeliverPoint add-in, provided by LightningTools, click **Open** and then click **OK**.

[<< Installation and Configuration of the DeliverPoint Add-In](#)
[Create Windows Azure Application >>](#)

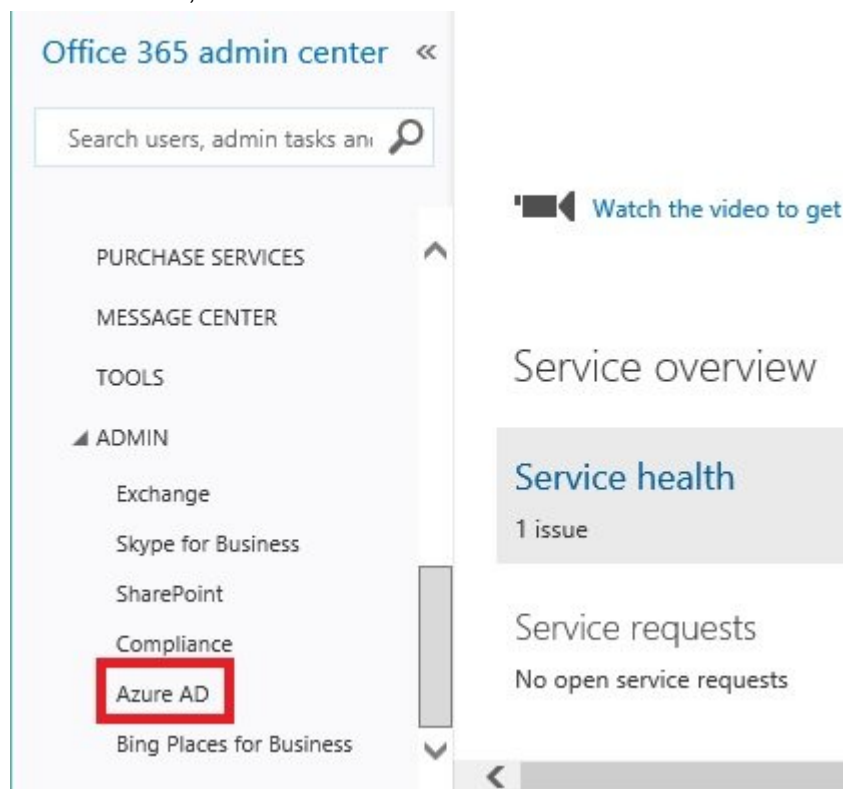
Create Windows Azure Application

When an Office 365 tenant is created, a Windows Azure Active Directory (WAAD) is created to store your [Office 365 user accounts and groups](#). You will usually manage your Office 365 users and groups using the Office 365 admin center, however you could manage your users and groups through the Windows Azure management portal or [Windows PowerShell](#). Also, the Azure management portal can be used to extend the capabilities of your Office 365 service, such as, [making an app appear on the Office 365 app launcher](#) or [integrating applications](#) in your Windows Azure Active Directory. If you upgrade your free subscription to Azure Active Directory to the premium edition more advanced capabilities are available, such as the advance application usage reporting.

In the case of the DeliverPoint add-in, consent must be given to allow access to the Azure Active Directory data. You do not need the premium edition of Azure Active Directory to complete the following steps:

1. Navigate to the [Windows Azure Management portal](#):

- From the [Office 365 admin centre](#):
 - Scroll down the Quick Launch
 - Under **Admin**, click **Azure AD**.



or

- Enter the following web address into your browser, <https://manage.windowsazure.com/>.

Tip: If you have never signed on to the Azure portal before, you will need to activate your free subscription and complete a one-time registration process. There are some links in the [Reference](#) and [Videos](#) sections at the bottom of this page you might find useful.

3. On the **All Items** page, click the name that represents your Office 365 tenant.

NAME	TYPE
Penny Coventry	Directory
PPP Consulting Ltd	Directory
P3C	Directory

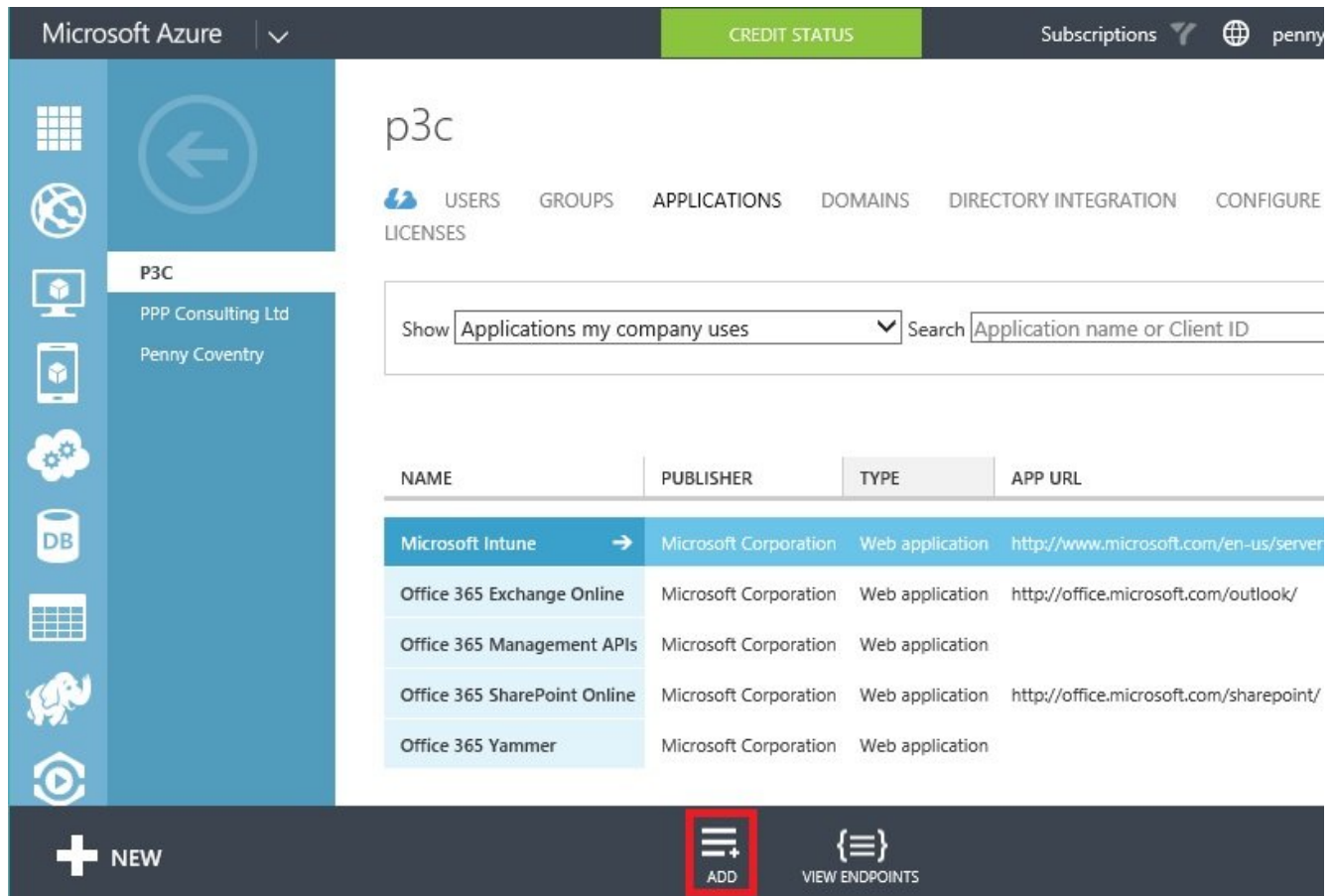
4. On the top menu, click **Applications**.

Microsoft Azure

p3c

USERS GROUPS APPLICATIONS DOMAINS

5. On the bottom menu, click **Add**.



The screenshot shows the Microsoft Azure portal interface for a tenant named 'p3c'. The top navigation bar includes 'Microsoft Azure', 'CREDIT STATUS', 'Subscriptions', and a user profile 'penny'. The left sidebar contains various service icons. The main content area shows tabs for 'USERS', 'GROUPS', 'APPLICATIONS', 'DOMAINS', 'DIRECTORY INTEGRATION', and 'CONFIGURE'. Below these is a search bar with a dropdown menu set to 'Applications my company uses' and a search input field. A table lists several applications, including Microsoft Intune, Office 365 Exchange Online, Office 365 Management APIs, Office 365 SharePoint Online, and Office 365 Yammer. At the bottom, a dark navigation bar contains a '+ NEW' button, a red-bordered 'ADD' button, and a 'VIEW ENDPOINTS' button.

NAME	PUBLISHER	TYPE	APP URL
Microsoft Intune	Microsoft Corporation	Web application	http://www.microsoft.com/en-us/server
Office 365 Exchange Online	Microsoft Corporation	Web application	http://office.microsoft.com/outlook/
Office 365 Management APIs	Microsoft Corporation	Web application	
Office 365 SharePoint Online	Microsoft Corporation	Web application	http://office.microsoft.com/sharepoint/
Office 365 Yammer	Microsoft Corporation	Web application	

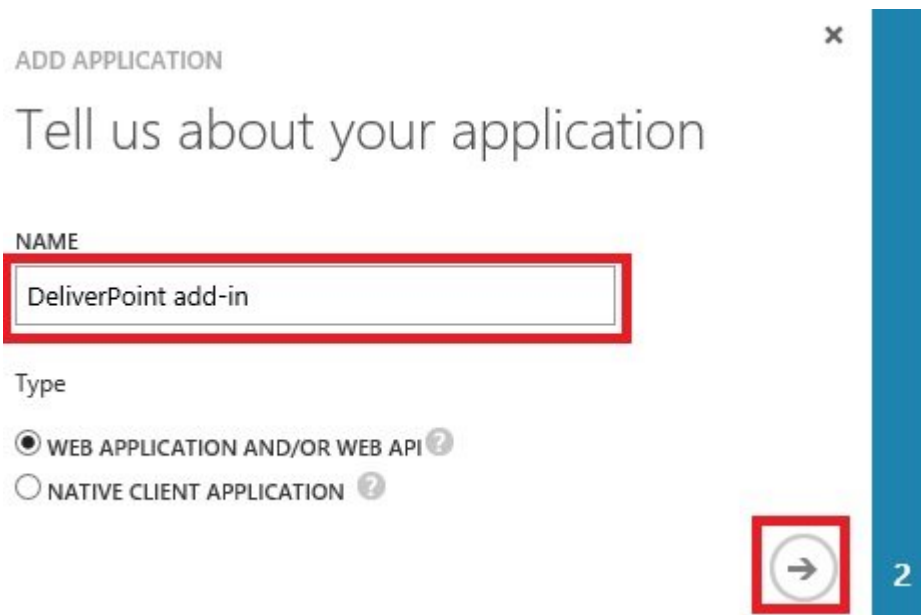
6. On the first page of the dialog, **What do you want to do**, click **Add an application my organization is developing**.

What do you want to do?

➔ Add an application my organization is developing

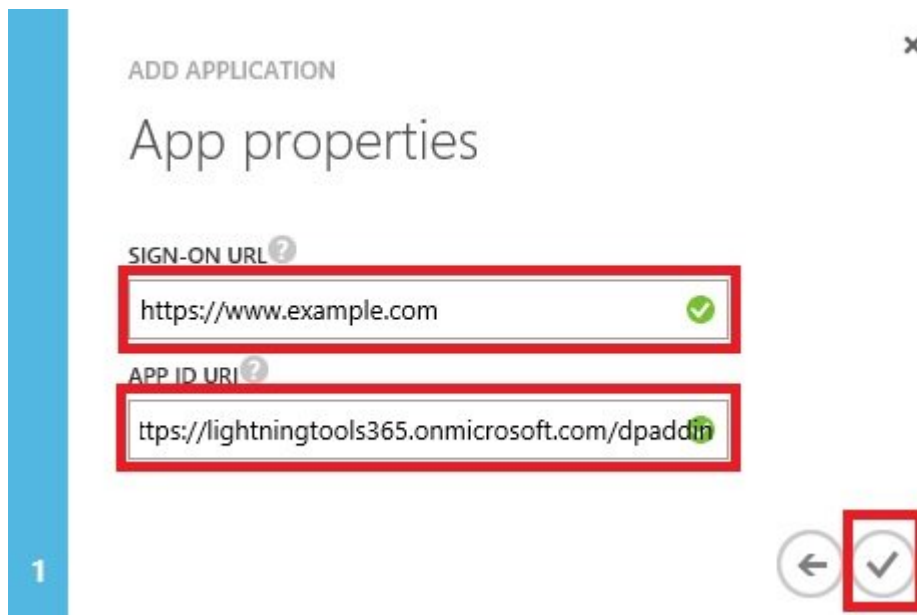
➔ Add an application from the gallery

7. On the **Tell us about your application** dialog page:
- In the **Name** text box, type a name, such as, [DeliverPoint add-in](#).
 - Click the right arrow.



8. On the **Add Properties** dialog page:

- In the **Sign-on URL** text box, type a web address, such as, <https://www.example.com>. This web address is not used by the DeliverPoint add-in and can be any web address.
- In the **App Id URI** text box, type the URL of your Office 365 tenant with an app name, such as, <https://lightningtools365.onmicrosoft.com/dpaddin>, where *lightningtools365.onmicrosoft.com* is the tenant web address, and *dpaddin* is the app name, which has to be unique within your Office 365 Azure Active Directory.
- Click the check icon.



ADD APPLICATION

App properties

SIGN-ON URL ?

✓

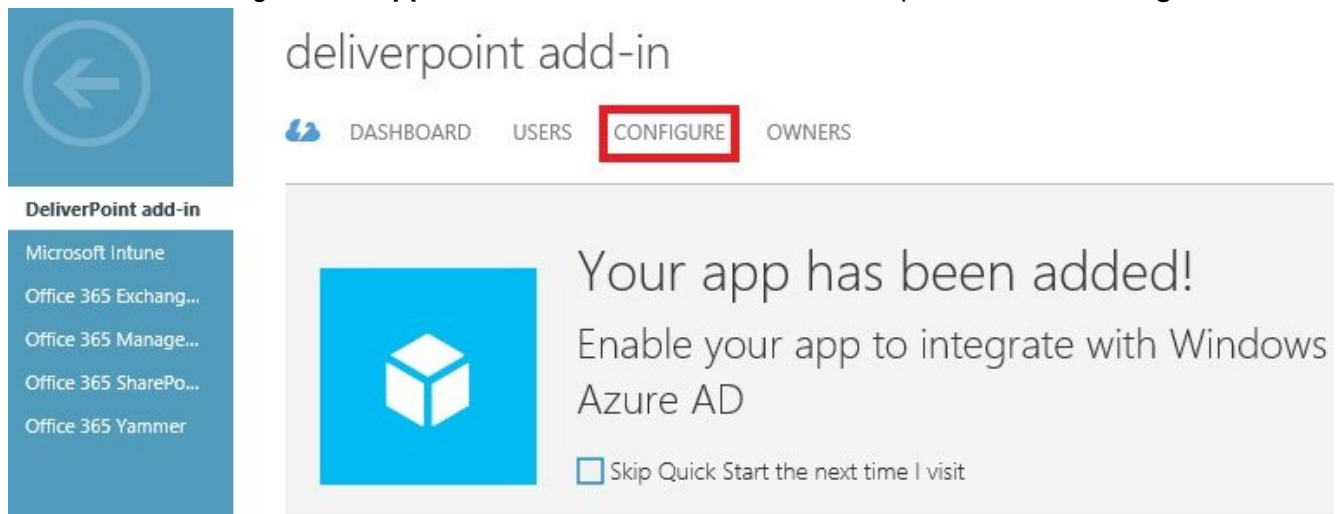
APP ID URI ?

✓

1

⏪ ✓

9. Wait for the message, **Your app has been added** and then on the top menu, click **Configure**.




deliverpoint add-in

⚡ DASHBOARD USERS **CONFIGURE** OWNERS

DeliverPoint add-in

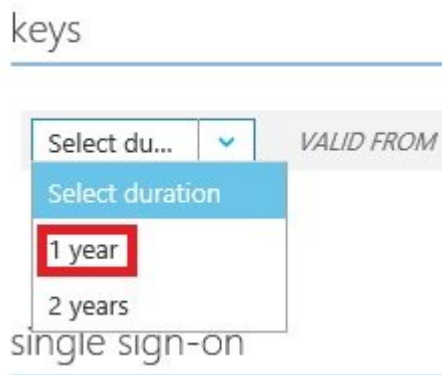
- Microsoft Intune
- Office 365 Exchang...
- Office 365 Manage...
- Office 365 SharePo...
- Office 365 Yammer

 Your app has been added!

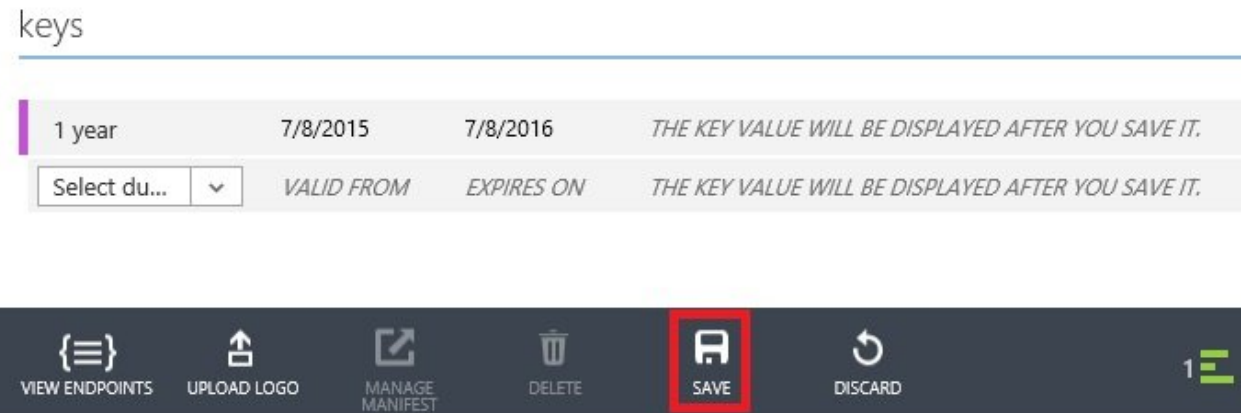
Enable your app to integrate with Windows Azure AD

☐ Skip Quick Start the next time I visit

- In the **Keys** section, from the **Select duration** menu, click **1 year**.



- On the bottom menu, click **Save** to display the key.



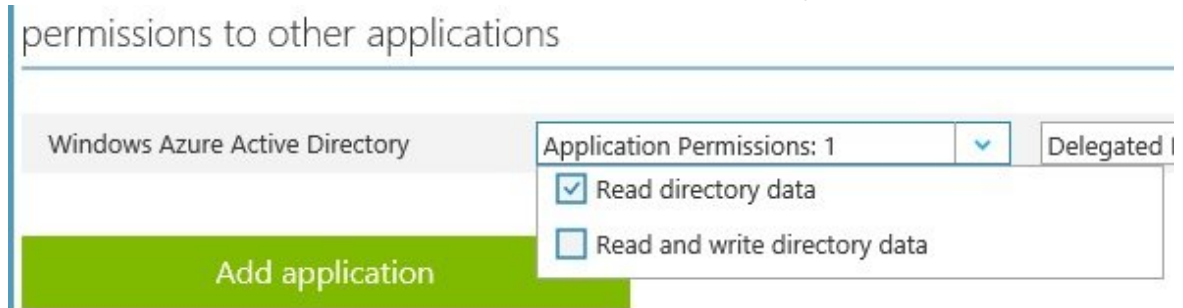
Wait for the operation to complete.

- Save both the **Client ID** and the year key you have just created, for example, in a text file. You will need both these values to configure the DeliverPoint add-in.

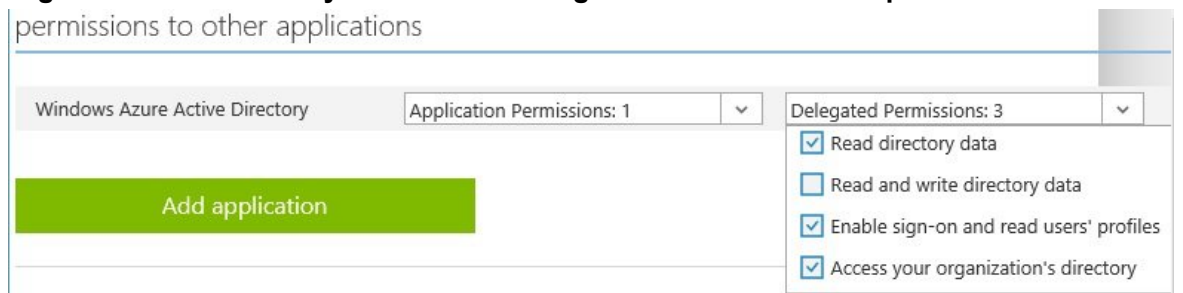
Tip: You will not be able to retrieve the 1 year key, once you leave the page. If you do not save the key you will need to generate a new one.

- In the **Permissions to other Applications** section to the right of **Windows Azure Active Directory**:

- In the **Application Permissions** menu, select **Read directory data**.



- In the **Delegated Permissions** menu, select **Read directory data** and **Access your organization's directory**. Leave **Enable sign-on and read user's profile** selected.



- On the bottom menu, click **Save** and wait for the updating of the configuration for the app to complete.

10. Close the Azure management portal browser window.

[<< Upload Add-In to App Catalog](#)

[Adding the Add-In to a Site >>](#)

References

- [Understanding Office 365 identity and Azure Active Directory](#)
- [Azure Active Directory editions](#)
- [Administering your Azure AD directory](#)

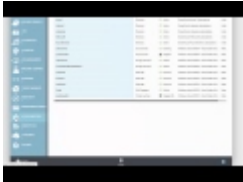
Videos

Accessing the Azure AD admin portal requires different steps depending on whether you have a trial Office 365 subscription or a paid Office 365 subscription.

- How to access the Azure portal for a paid Office 365 subscription.



- How to access the Azure portal for a trial Office 365 subscription.




- [Windows Azure Active Directory – Common Sign-up, sign-in and usage questions](#)
- [Office 365 identity just got easier – new options and tools for Azure AD](#)
- [Azure AD Connect Health : Monitor your identity bridge](#)

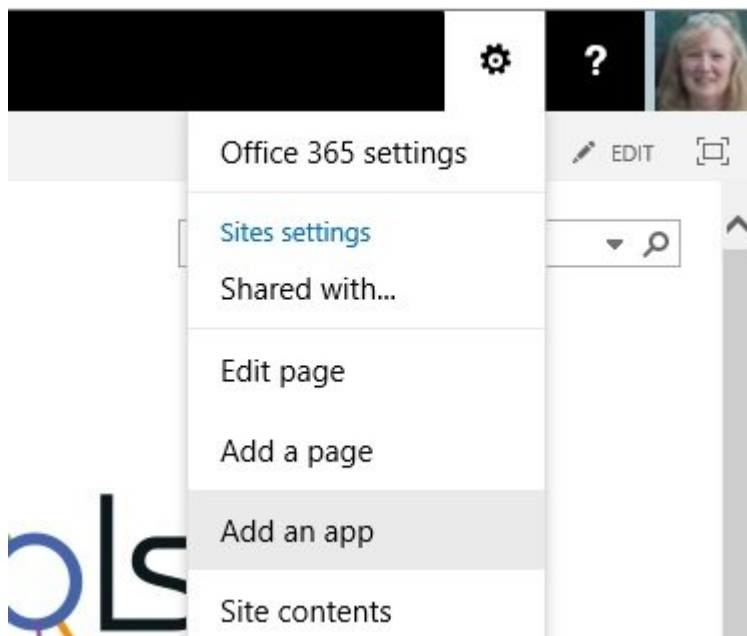
Adding the Add-In to a Site

To use the DeliverPoint Add-In, you first need to add the DeliverPoint Add-In to a site in the site collection where you want to create a discover permissions report. There are many ways of [adding an Add-In to a site](#). The steps in this section, assume that the *DeliverPoint* Add-In appears under *From Your Organization* in the *App Catalog*. To add the *DeliverPoint* Add-In to the *App Catalog*, use the steps documented in the [Installation of Add-In](#) section of this online manual.

To add the [DeliverPoint Add-In](#) to a site, use the following steps. :

! You need to be mapped to the Full Control [permission level](#) to complete the following steps. If you are a Site Owner, then you will be mapped to this permission level.

1. Navigate to the site where you wish to use the DeliverPoint Add-In.
2. Click **Settings**  in the top right corner of the team site, and then click **Add an app**.



3. On the **Your Apps** page, under **Apps you can add**, click **DeliverPoint**.

Tip: In your organization you may find the *DeliverPoint* add-in below **Noteworthy**. If your organization

has many apps, to quickly find the app, type **DeliverPoint** in the **Find an app** search box.

4. On the **Do you trust DeliverPoint** dialog, click **Trust It**.

The *Site Contents* page is displayed, and the app will begin to install. It will first appear grayed during the installation, and then when the installation is complete you will see the DeliverPoint add-in.

You can now start to use the Add-In, as described in the in the [Using the Add-in](#) section of this online manual.

[<< Create Windows Azure Application](#)

[Configure DeliverPoint Add-In >>](#)

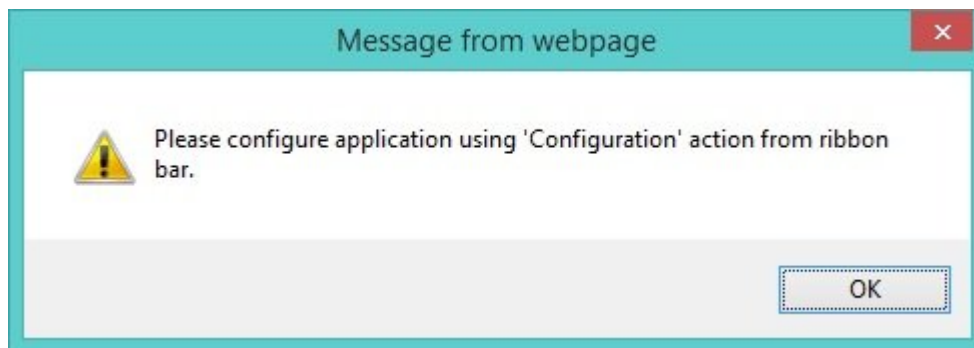
Related Office.com documentation

- [Add an app to a site →](#)
- [Monitor apps for a site →](#)
- [Remove an app from a site →](#)
- [Permissions in Office 365 →](#)
- [Introduction: Control user access with permissions →](#)
- [Understanding permission levels →](#)

Configure DeliverPoint Add-In

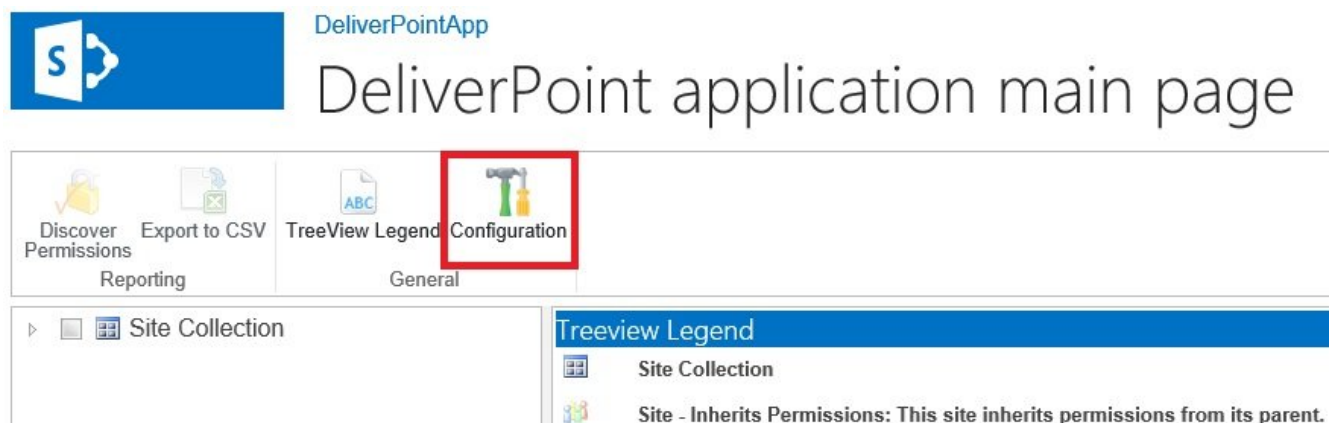
Before you can use the DeliverPoint Add-In, it must be configured with the Office 365 tenant domain, and the client id and secret key that was created when the [Windows Azure application was created](#). Once you have those three pieces of information, complete the following steps:

1. Navigate to a site where you have added the DeliverPoint Add-In.
2. From the Quick Launch or the site contents page, click **DeliverPoint**.
3. If a dialog box is displayed, stating to *Please configure the application, using the 'Configuration' command on the Ribbon*, click **OK**.



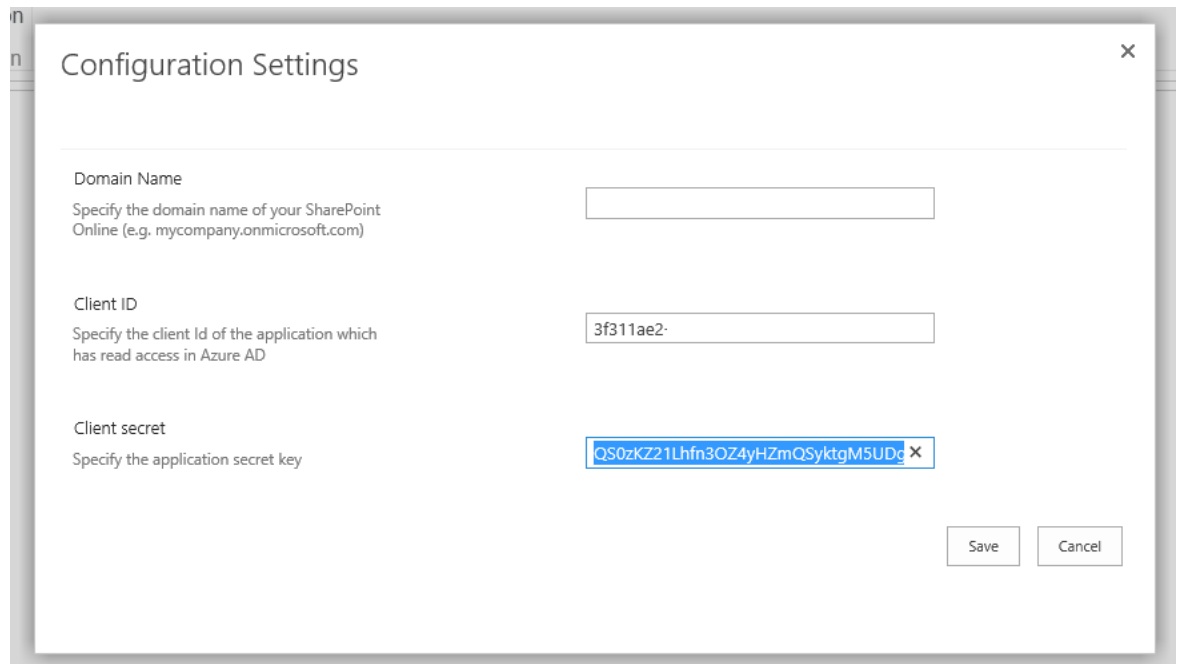
The DeliverPoint application main page is displayed.

4. On the Ribbon, click **Configuration** in the **General** group.



5. In the **Configuration Settings** dialog:

- In the Domain Name text box, type the domain name of your Office 365 tenant, for example, lightning365.onmicrosoft.com
- In the **Client ID** text box, type the Client ID of the Azure application you saved previously.
- In the **Client secret** text box, type the Key of the Azure application you previously saved.



The image shows a 'Configuration Settings' dialog box with three input fields. The first field is 'Domain Name' with a placeholder 'Specify the domain name of your SharePoint Online (e.g. mycompany.onmicrosoft.com)'. The second field is 'Client ID' with a placeholder 'Specify the client Id of the application which has read access in Azure AD' and contains the value '3f311ae2'. The third field is 'Client secret' with a placeholder 'Specify the application secret key' and contains the value 'QS0zKZ21Lhfn3OZ4yHZmQSyktgM5UDg'. There are 'Save' and 'Cancel' buttons at the bottom right.

Field	Value
Domain Name	
Client ID	3f311ae2
Client secret	QS0zKZ21Lhfn3OZ4yHZmQSyktgM5UDg


- Click **Save**.

[<< Adding the Add-In to a Site](#)

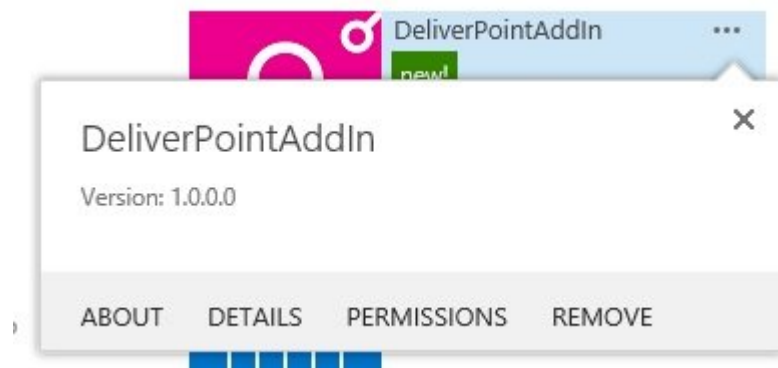
[How to tell the version of the Add-In >>](#)

How to tell the version of the Add-In

To find the version of the DeliverPoint Add-In complete the following:

1. Navigate to a site where you have [added the DeliverPoint add-in](#).
2. Either on the Quick Launch click **Site Contents** or from the **Setting**  menu, click **Site Contents**.
3. Point to the tile for the DeliverPoint Add-In, and click the ellipse (...) next to the add-in name.

A callout displays which contains version information.



The DeliverPoint callout provides the following links.

- **About.** Use to display the DeliverPoint page on the SharePoint Store.
- **Details.** Use to display the **App Details** page, which allows a site owner to monitor information about the Add-In, for example, you can view information about how often the Add-In has been launched and how many errors the Add-In has had. For more information of this option, see the Microsoft Office support page, [Monitor apps for a Site](#).
- **Permissions.** Use to display the permissions of the DeliverPoint Add-In.
- [Remove.](#) Use this link if you no longer need the DeliverPoint Add-In on your site.


Note: To [remove an Add-In](#), you must have Full Control permissions for the SharePoint site. If you are a Site Owner, you are mapped to this permission level.

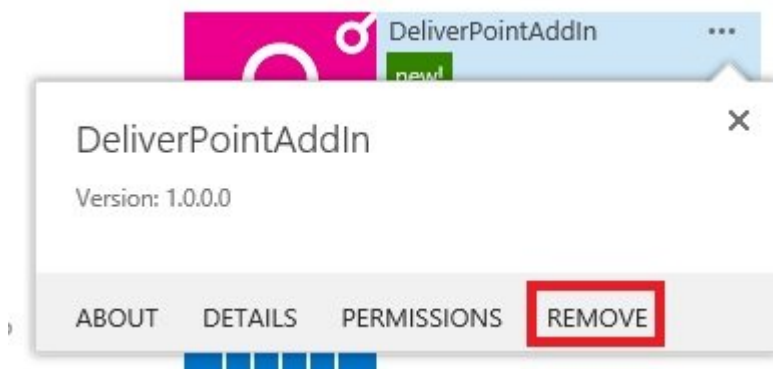
[<< Configure DeliverPoint Add-In](#)
[Removing the Add-In from a site >>](#)

Removing the Add-In from a site

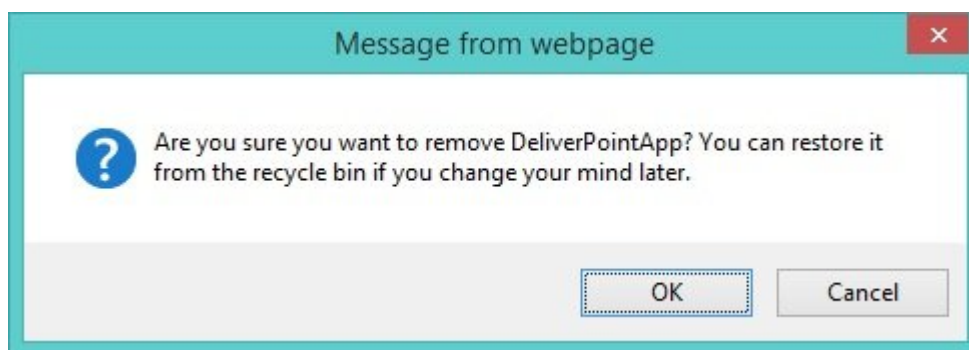
To remove the [DeliverPoint Add-In](#) from a site, use the following steps. :

! You need to be mapped to the Full Control permission level to complete the following steps. If you are a Site Owner, then you will be mapped to this permission level.

1. Navigate to the site where you wish to remove the DeliverPoint Add-In.
2. Either, on the Quick Launch, click **Site Contents** or from the **Settings**  menu click **Site Content**.
3. On the *Site Contents* page, point to the tile for the DeliverPoint Add-In, click the ellipse (...) next to the Add-In name and then click **Remove**.



4. Click **OK** to close the dialog box asking you if you are sure you want to remove the Add-In.



The Add-In is removed from the site, and placed in the recycle bin.

Note: If you try to add the Add-In once it is removed, you may see an error that you may need to delete the Add-In from the site and the site collection recycle bin to install the Add-In. Instructions on how to delete an Add-In from the recycle bins are documented next on this page.



Although you can restore the Add-In from the recycle bin, permissions to the Add-In will not be configured correctly and no one will be allowed access to the Add-In. Therefore if you need to use the Add-In again on a site, you should always delete the Add-In from the both the end user's and second-stage recycle bins, if it still exists there, and then [add the DeliverPoint Add-In](#).

To delete the Add-In from the recycle bin, use the following steps:

1. Navigate to the site where you removed the DeliverPoint Add-In.
2. Either, on the Quick Launch, click **Recycle Bin** or from the **Site Contents** page click **Recycle Bin**.
3. On the *Recycle Bin* page, select the check box to the left of the Add-In, and then click **Delete Selection**.

Note: The Add-In, unless deleted from the recycle bin, will remain in the end user's recycle bin for 30 days.

4. Click **OK** to close the dialog box, *Are you sure you want to remove "DeliverPoint from the end user's Recycle Bin"*.
5. At the bottom of the *Recycle Bin* page, click **second-stage recycle bin**.
6. On the *Second-Stage Recycle Bin* page, select the check box to the left of the Add-In, and then click **Delete Selection**.
7. Click **OK**, to close the dialog box, *Are you sure you want to permanently delete this item*.

Note: The Add-In, once deleted from the end user's recycle bin, remains in the second-stage recycle bin for 93 days, unless the previous step is completed.

References

- [Manage the Recycle Bin of a SharePoint Online site collection](#)
- [Empty the recycle bin or restore your files](#)

[<< How to tell the version of the Add-In](#)

[Using the Add-in >>](#)

Using the Add-in

At the moment, the DeliverPoint add-in only provides reporting of permissions ([discover permissions](#)) within your Microsoft® SharePoint® Online [Office 365™](#) tenant.

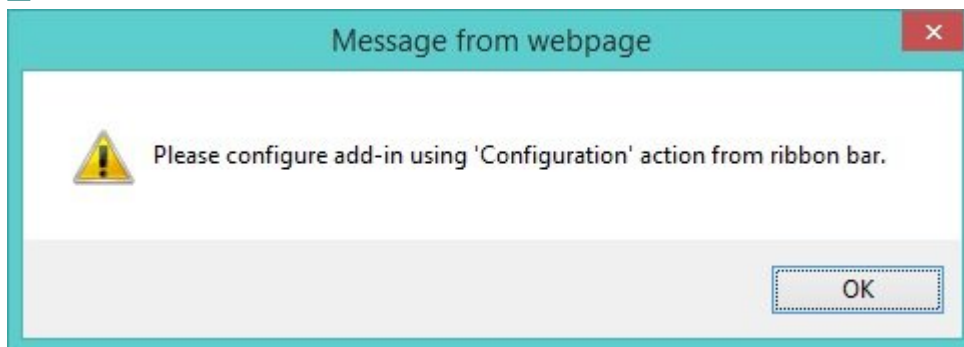
- * Users can only use the DeliverPoint [Discover Permission](#) action if they have the SPBasePermission Enumerate permission, that is, only users who have access to view permissions in SharePoint can access this DeliverPoint action. For example, users who are mapped to a permission level that includes the Manage Permissions right, such as, Full Control, will be able to use this action.

You can use the DeliverPoint add-in to manage permissions, at the [top level site of a site collection](#), [site](#), [list/library](#) and [list item/file](#) levels.

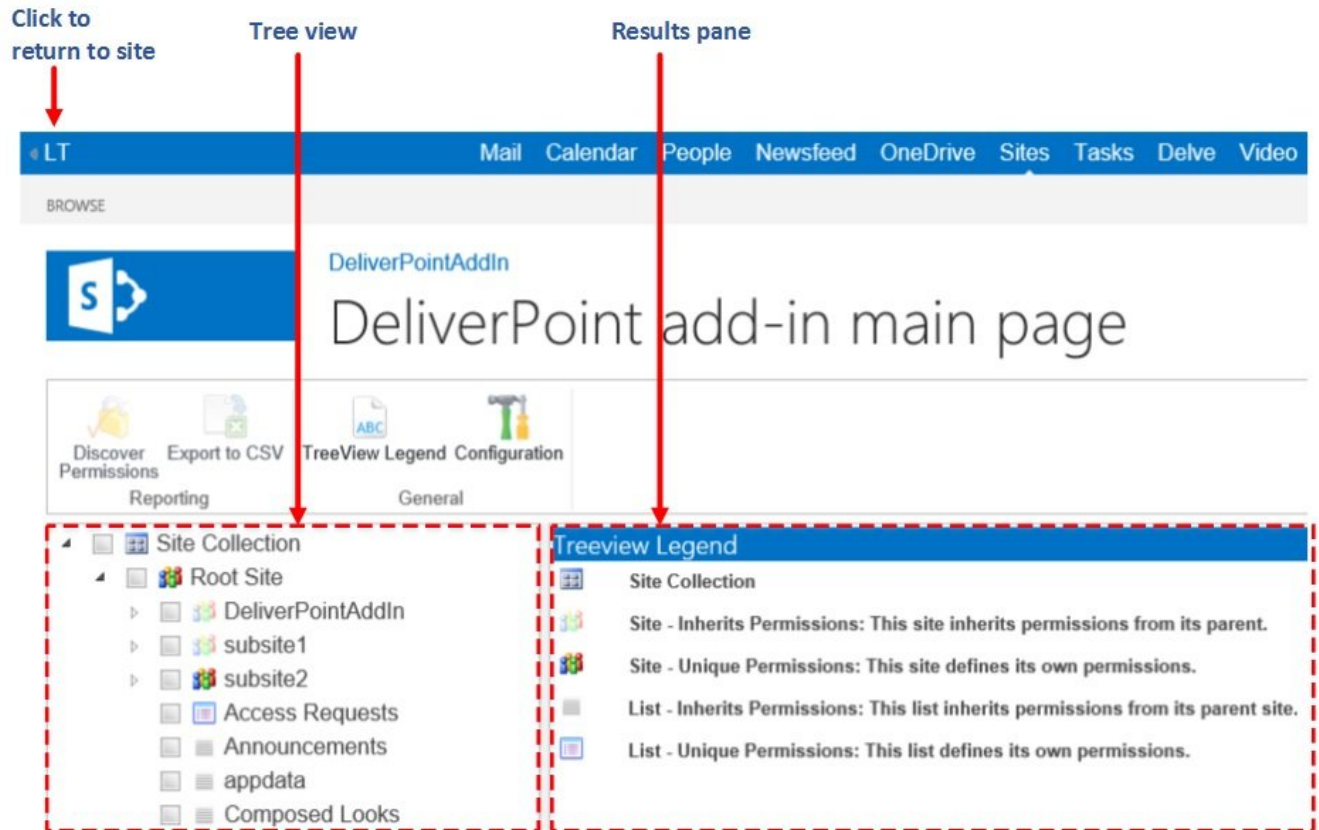
Site, list and library permission management

To complete site collection, site, list or library levels you use the DeliverPoint add-in main page. To navigate to the DeliverPoint add-in main page, complete the following steps:

1. Navigate to a site where you have added the DeliverPoint add-in.
2. From the Quick Launch or the site contents page, click **DeliverPoint**.
3. If a dialog box is displayed, stating to please configure the application, using the Configure action on the Ribbon, click **OK**, and then complete the steps described in the [Configuring the DeliverPoint Add-in](#) section.



The DeliverPoint add-in main page is displayed.

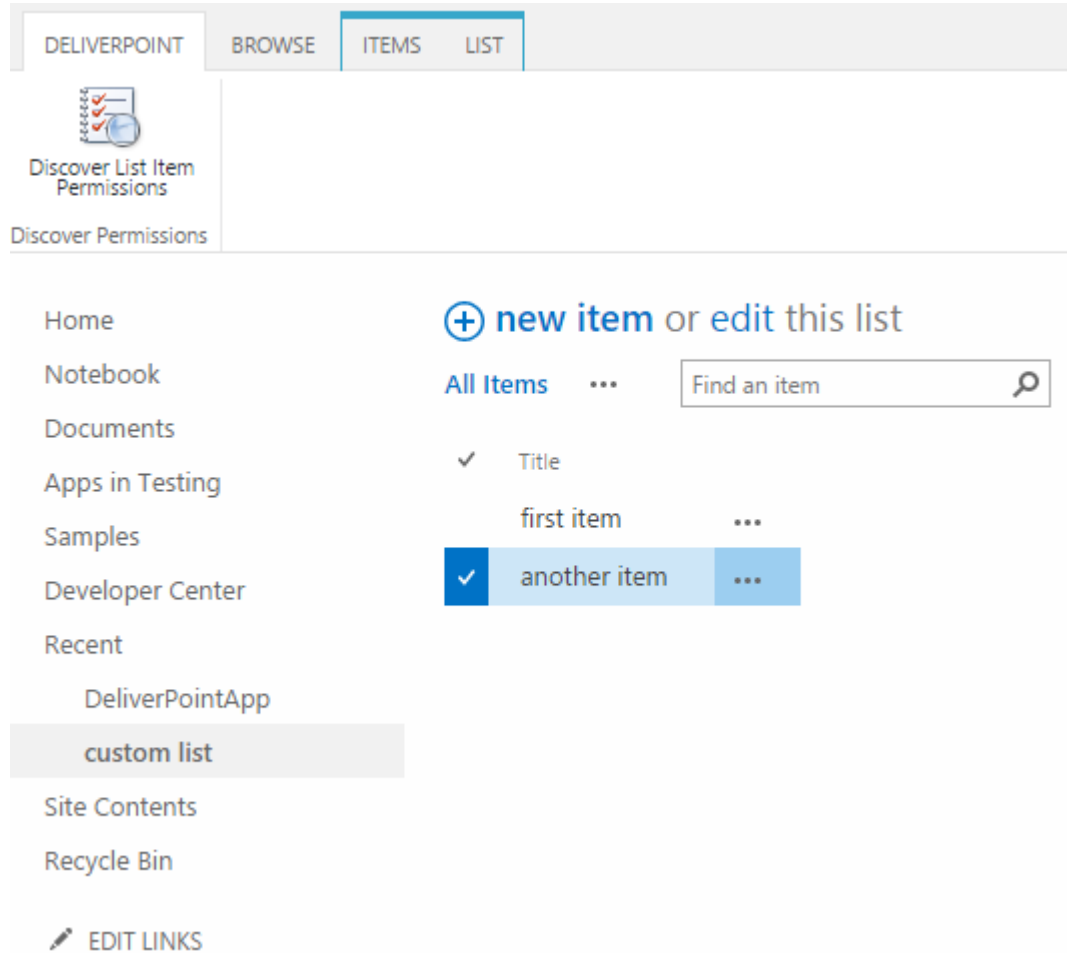


The DeliverPoint add-in main page consists of:

- **Ribbon.** This contains the commands to complete the following actions:
 - [Discover Permissions](#). Allows the user to find out who has access to a given object and how that access is given.
 - **Export to CSV.** Allows you to export the results to a comma-separated values (CSV) file, which you could then open in a program, such as, Microsoft® Excel to analysis the data.
 - **TreeView Legend.** Displays a [legend of the icons](#) used in the Tree view area.
 - **Configuration.** Use to [configure the DeliverPoint add-in](#).
- **Tree view** pane. The tree view area, displays the site collection, the sites within the site collection and the lists and libraries within each site that you have permissions to view. You will use the check box to the left of each SharePoint object displayed to identify which object to complete the permission management task.
- **Results** pane. As you complete different DeliverPoint tasks, the results pane is used to display the results of those tasks. When you first display the DeliverPoint add-in main page, the result pane displays the legend of the icons that appear in the tree view.
- **Selected Scope** pane. This pane is displayed at bottom of the DeliverPoint add-in main page and displays the SharePoint object selected in the tree view pane.






List item and file permission management

On sites where you have added the DeliverPoint add-in, you can complete DeliverPoint permission management task on list items and files. Lists and libraries in sites where the DeliverPoint add-in has been added will display a the DeliverPoint Ribbon tab.



[<< Removing the Add-In from a site](#)
[Add-in Tree View Legend >>](#)

Add-in Tree View Legend

Icon	Description
	Site collection
	Site that inherits permissions from parent site. When you create a subsite, the default is always to inherit its permissions from the parent site.
	Site with unique permissions, that is, the site does not inherit its permissions from a parent site. The site defines its own permissions. The top-level site of a site collection is always a site with unique permissions.
	List that inherits permissions from the parent site. When you create a list or library, the default is always to inherit its permissions from the parent site.
	List with unique permissions, that is, the list or library does not inherit its permission from a parent site. The list or library defines its own permissions.

[<< Using the Add-in](#)

[Discover permissions using the add-in >>](#)

Discover permissions using the add-in

‘Discover who has permissions to this SharePoint object’

Discover Permissions allows the user to find out who has access to a given object and how that access is given. You can only use the Discover Permission DeliverPoint action if you have the SPBasePermission Enumerate permission, that is, only users who have access to view permissions in SharePoint can access this DeliverPoint action. For example, users who are mapped to a permission level that includes the Manage Permissions right, such as, Full Control, will be able to use this action.

There are three levels of the Discover Permissions:

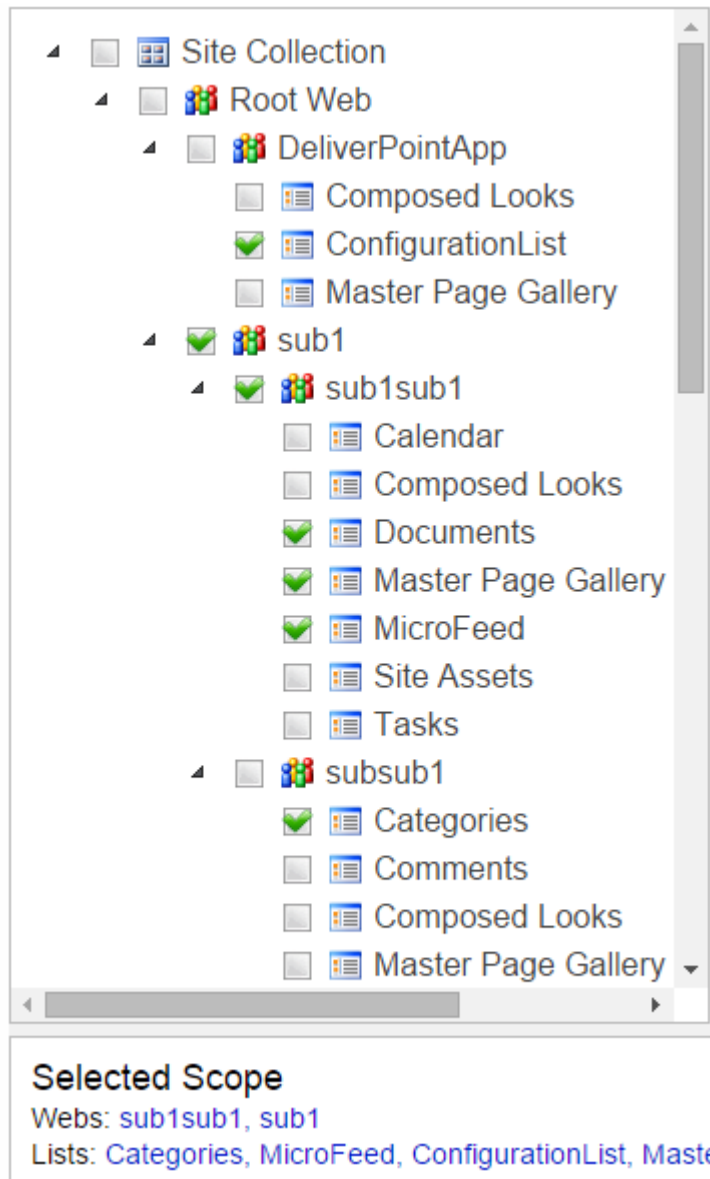
- [Discover Site Permissions](#)
- [Discover List Permissions](#)
- [Discover Item Permissions](#)

All three forms of this DeliverPoint action uses the Discover Permissions with [DeliverPoint add-in main page](#) to display the [results](#), which you can use to [filter the results](#). The Discover Permissions report and how to filter the results are explained in the next section.

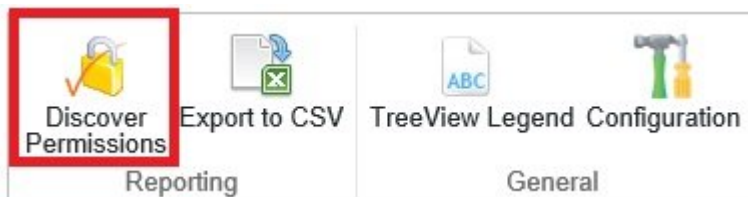
Discover Site and List Permissions

1. [Display the DeliverPoint add-in main page](#).
2. In the left hand navigation, expand the tree view and select the check boxes to the left of the required SharePoint object(s).

Tip: The order you select the objects affects the order that the objects are displayed in the report. Subsites and list and libraries will only appear in the report if selected, that is, by selecting the top level site in a site collection, only the configuration at the site level are reported.



3. On the Ribbon, click **Discover Permissions** in the **Reporting** group.



The Discover Permissions report is displayed in the results pane of the DeliverPoint add-in main page.

The screenshot displays the Lightning Tools interface with a left-hand navigation pane and two main content areas. The left pane shows a site collection structure with 'Root Site' expanded, listing various components like 'DeliverPointAdd', 'subsite1', 'subsite2', 'Access Request', 'Announcements', 'appdata', 'Composed Look', 'Content type pul', 'Converted Form', 'Documents', 'Form Templates', 'List Template Ga', 'Master Page Ga', 'MicroFeed', 'Pay Discussions', 'Project Policy It', 'Site Assets', 'Site Pages', 'Solution Gallery', 'Style Library', 'TaxonomyHidde', 'Theme Gallery', 'User Information', 'Web Part Gallen', and 'wfpub'. The 'Pay Discussions' list is highlighted.

The top content area, titled 'Site permissions', shows a table of permissions for the selected scope (LT). The bottom content area, titled 'List permissions', shows a table of permissions for the selected list (Pay Discussions).

Scope	User	Permission	Via
LT	ltadmin o365	Full Control	LT Owners
LT	ltadmin o365	Limited Access	LT Owners
LT	Penelope Coventry	Full Control	LT Owners
LT	Penelope Coventry	Limited Access	LT Owners
LT	System Account	Full Control	LT Owners
LT	System Account	Limited Access	LT Owners
LT	visitor1 o365	Read	LT Visitors
LT	admin o365	Edit	LT Members
LT	user1 o365	Edit	LT Members
LT	user2 o365	Edit	LT Members
LT	user1 o365	Limited Access	g_users
LT	user2 o365	Limited Access	g_users

Parent Site	Scope	User	Permission	Via
LT	Pay Discussions	ltadmin o365	Full Control	LT Owners
LT	Pay Discussions	ltadmin o365	Limited Access	LT Owners
LT	Pay Discussions	Penelope Coventry	Full Control	LT Owners

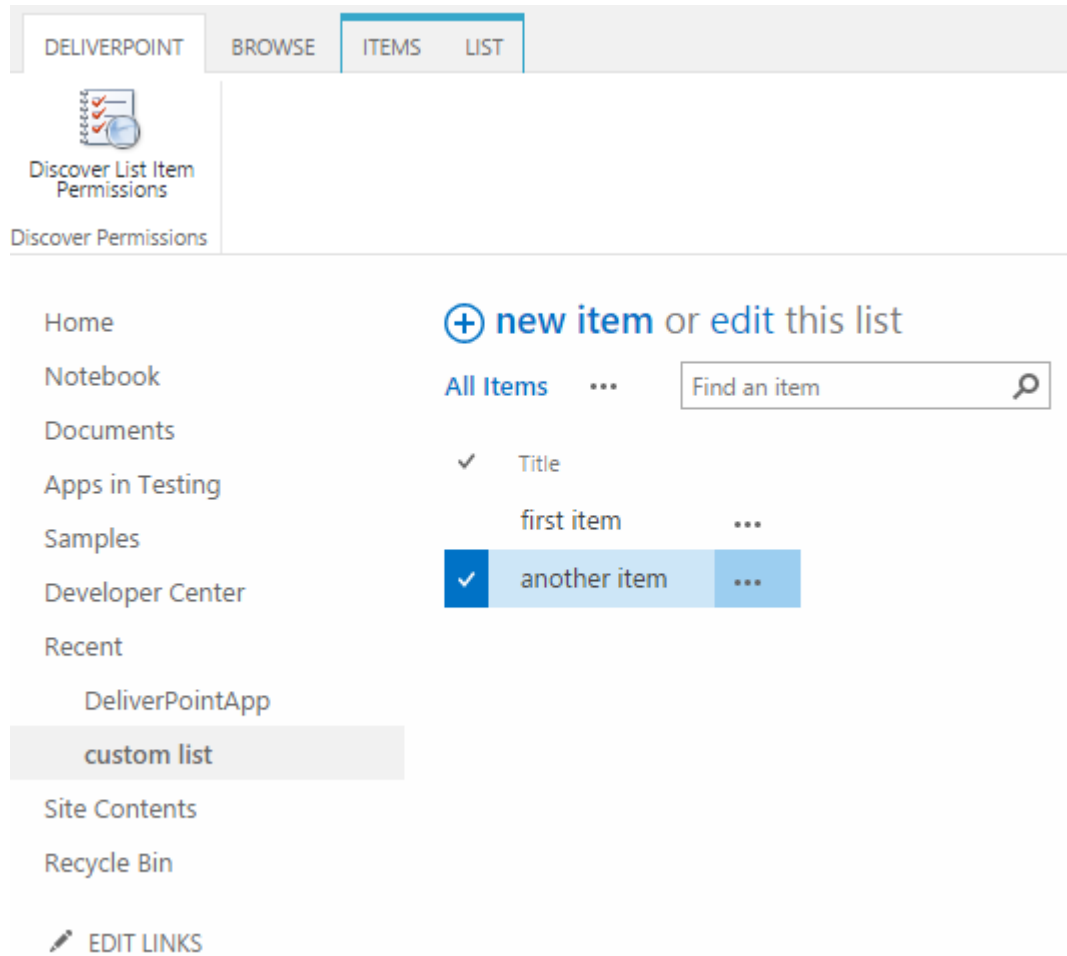
Selected Scope
 Sites: [Root Site](#)
 Lists: [Pay Discussions](#)

In the bottom pane, the SharePoint objects that were selected to create the report are listed, for example, in the above screen shot the top level site of the site collection (LT) and the list Pay Discussions where selected.

- To return to the home page of your SharePoint site, click the link in the top left corner.

Discover Item Permissions

On sites where you have [added the DeliverPoint add-in](#), lists and libraries will display a the DeliverPoint Ribbon tab.



1. Select the check box to the left of the list items or files to include in the report.
Tip: When no items are selected, all items will be included in [Discover Permissions report](#).
2. On the DeliverPoint Ribbon tab click **Discover List Item Permissions**.

The [Discover Permissions results](#), allows you to [filter](#) the results.

References

[<< Add-in Tree View Legend](#)
[Discover Permissions add-in report >>](#)

Discover Permissions add-in report

The [Discover Permissions](#) report is displayed in the results pane of the [DeliverPoint add-in main page](#). The results are batched into SharePoint object type, that is, site, list/library and list item/file. Only 20 results are displayed per each object type and at the bottom of each object type section there are page numbers you use to display the next or previous set of 20 results.

The screenshot displays the 'Discover Permissions' report interface. On the left is a 'Site Collection' tree with 'Root Site' expanded, showing various site components like 'DeliverPointAdd', 'subsite1', 'subsite2', 'Access Request', 'Announcements', 'appdata', 'Composed Look', 'Content type pul', 'Converted Form', 'Documents', 'Form Templates', 'List Template Ga', 'Master Page Ga', 'MicroFeed', 'Pay Discussions', 'Project Policy It', 'Site Assets', 'Site Pages', 'Solution Gallery', 'Style Library', 'TaxonomyHidde', 'Theme Gallery', 'User Information', 'Web Part Gall', and 'wfpub'. The main area is divided into two sections: 'Site permissions' and 'List permissions'.

Site permissions table:

Scope	User	Permission	Via
LT	ltadmin o365	Full Control	LT Owners
LT	ltadmin o365	Limited Access	LT Owners
LT	Penelope Coventry	Full Control	LT Owners
LT	Penelope Coventry	Limited Access	LT Owners
LT	System Account	Full Control	LT Owners
LT	System Account	Limited Access	LT Owners
LT	visitor1 o365	Read	LT Visitors
LT	admin o365	Edit	LT Members
LT	user1 o365	Edit	LT Members
LT	user2 o365	Edit	LT Members
LT	user1 o365	Limited Access	g_users
LT	user2 o365	Limited Access	g_users

List permissions table:

Parent Site	Scope	User	Permission	Via
LT	Pay Discussions	ltadmin o365	Full Control	LT Owners
LT	Pay Discussions	ltadmin o365	Limited Access	LT Owners
LT	Pay Discussions	Penelope Coventry	Full Control	LT Owners

At the bottom, the 'Selected Scope' section shows: Sites: [Root Site](#), Lists: [Pay Discussions](#).

The page contains the following columns:


- **Scope.** When the hyperlink is clicked the home (default) page of the site / list or the property page of the list item / file is displayed.
- **User.** The account's Display Name.
- **Permission.** the permission level(s) that is mapped to the account on the object.
- **Via.** Lists graphically how the user has been given access to the object. To expand SharePoint Groups or Active Directory group, click the plus sign (+) to the left of the group name.

- **Parent Site.** When the SharePoint object selected is a list/library or list item/file then this column displays the site where the SharePoint object is stored.

Sorting the results

You can sort the results using the column headings **Scope**, **User**, **Permission** and **Via**. When a report is first displayed the results are displayed in the order the SharePoint objects were selected in the tree view. Sorting is completed against all the results returned, that is, sorting is not limited to the 20 results displayed on a specific page when there are more than 20 results are returned.

Filtering the results

The [Filter](#) icon  displayed to the right of each column heading can be used to refine the results returned. See the [next section](#) for more information on how to filter the results of the discover permission action.


Exporting the results

To export the results, click **Export to CSV** in the **Reporting** group on ribbon. If your browser is configured to block pop-ups, you may have to allow pop-ups to display the option to save the file. The file name is of the format, *ExportPermissions_yyyy-mm-ddThh_mm_ss1Z.csv*. All results are exported, that is, the results exported are not limited to the results displayed on a specific page when more than 20 results returned from the *Discover Permissions* command.




References



[<< Discover permissions using the add-in](#)
[Refining Discover Permissions add-in results >>](#)

Refining Discover Permissions add-in results

The [Discover Permission](#) add-in results can be customized, using the [Filter](#) icon  to the right of the column headings.


Column Heading Filtering

Use the *Filter* icon  displayed to the right of each column heading to filter the *Discover Permissions* results by *Scope*, *User*, *Permission* or *Via*. When a filter is configured for a column heading then the *Remove Filter* icon  is displayed to the right of the *Filter* icon .

When you click the *Filter* icon  a dialog box opens that allows you to configure one or more filter criteria. By default the *Filter By* dialog contains three drop down lists for you to configure one filter criteria, to add another criteria, select either **And** / **Or** and then click the green plus icon  :

- Click **And** to create a filter where the data must match the criteria in all filter criteria.
- Click **Or** to create a filter where the data must match the criteria in only one filter criteria.

Each criteria can be removed from the filter by clicking the remove filter icon .

Once the filter is configured click **Save**. To edit an existing filter, click the *Filter* icon  again.

References

[<< Discover Permissions add-in report](#)

DeliverPoint SharePoint Online Add-In for Office 365 Professional

DeliverPoint SharePoint Online Add-In for Office 365 Professional is an in-context Microsoft® SharePoint® Permissions Management Tool that enables SharePoint Office 365 site collection administrators the ability to effectively manage SharePoint permissions within the context of a SharePoint O365 environment. This tool differs from the [DeliverPoint SharePoint Online Add-In for Office 365](#) (non-Professional), in that it provides many permissions management features above and beyond the Discover Permissions operation, such as Copy, Grant, Transfer, and Delete Permissions, as well as options for managing [Permission Inheritance](#).



If you are new to managing permissions in SharePoint Online which comes with your [Office 365™](#) tenant, then you will find some useful links in the [References](#) section at the bottom of this page.

References

- [Introduction: Control user access with permissions](#)
- [Video: Understanding permissions in SharePoint](#)
- [Plan your permissions strategy](#)
- [Plan sites and manage users](#)
- [Plan your permissions strategy](#)
- [Governance: Permission Management](#)

[Installation and Configuration of the DeliverPoint Add-In >>](#)

Installation and Configuration of the DeliverPoint Add-In

This section details how to install the DeliverPoint SharePoint Online Add-In Office 365 Professional from [Lightning Tools](#), so it can be used to report on permissions within SharePoint® Online. The installation of the DeliverPoint Add-In is a four-step process:

- Install the Add-In by getting the Add-In from Lightning tools and [uploading it into your organization's Office 365 app catalog](#).
- Create an [Azure application](#) with access to your Office 365 domain and obtaining a client-id and secret key of the Azure application.
- [Add the Add-In](#) to a SharePoint site.
- [Configure the Add-In](#) with the tenancy domain URL, and the Azure Add-In client-id and secret key.

[<< DeliverPoint SharePoint Online Add-In for Office 365 Professional](#)
[Upload Add-In to App Catalog >>](#)


Upload Add-In to App Catalog

This section details how to install the DeliverPoint Add-In from [Lightning Tools](#), so it can be used on [Office 365™](#) sites. By completing the steps in this section, the DeliverPoint Add-In appear on the Your Apps page, under Apps you can add, for all sites within an [Office 365™](#) tenant.

! To use the following method to install the DeliverPoint add-in to an Office 365 tenant, you must be an [Office 365 global admin](#).

1. Obtain the Add-In from: [Lightning Tools](#)
2. Navigate to your [SharePoint admin center](#).

Note: If you are unsure where your [SharePoint admin center](#) site is:

- a. Click the [Apps Launcher](#)  icon in the top left and then click **Admin** to display the [Office 365 admin center](#).
 - b. At the bottom of the Quick Launch, expand **Admin** and then click **SharePoint** to display the *SharePoint admin center*.
3. On the Quick Launch, click **apps**, and then click **App Catalog** to display the home page of the App Catalog site.
 4. On the Quick Launch, click **Apps for SharePoint**.
 5. Click **Upload** to display the **Add a document** dialog.
 6. Click **Browse** to open the **Choose File to Upload** dialog box.
 7. Navigate to where you have stored the DeliverPoint add-in, provided by LightningTools, click **Open** and then click **OK**.

[<< Installation and Configuration of the DeliverPoint Add-In](#)
[Create Windows Azure Application >>](#)

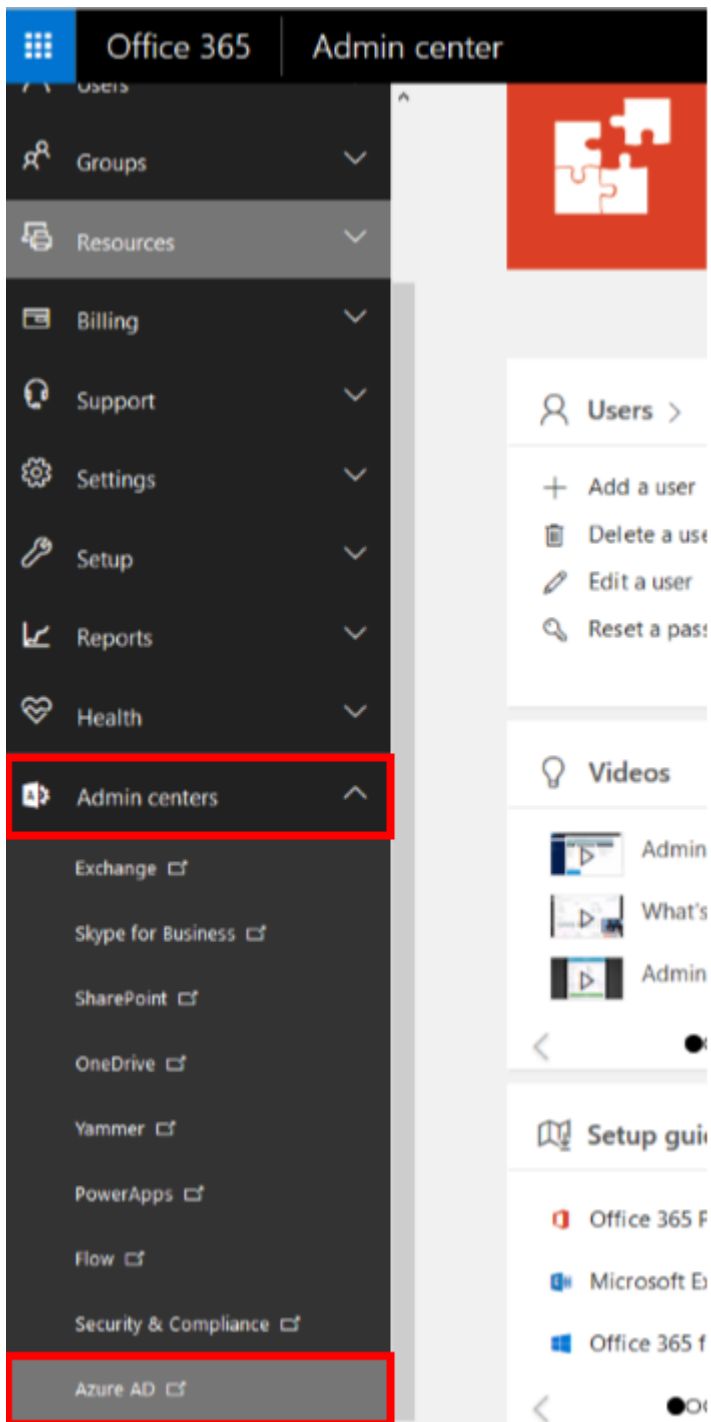
Create Windows Azure Application

When an Office 365 tenant is created, an Azure Active Directory (Azure AD) is automatically created to store all of your [Office 365 users accounts and groups](#). In most cases, you would usually manage your Office 365 permissions from the Office 365 Admin Center, however it is possible to manage your users and groups through Azure AD or [Windows PowerShell](#). You start with a free subscription of Azure AD, however you can upgrade to a premium version.

In the case of the DeliverPoint Add-in, consent to install the solution must be given, as the DeliverPoint Add-in needs access to the Azure AD data. You do NOT need the premium edition of Azure AD to install the DeliverPoint Add-in

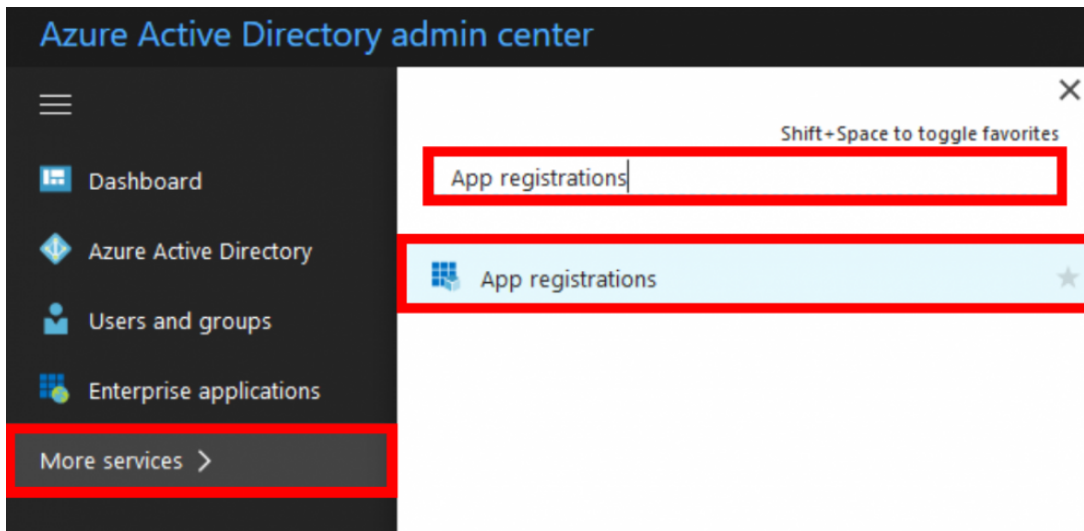
1. Navigate to the **Azure Active Directory Admin Center**:

From the **Office 365 Admin Center**, scroll down the navigation menu, under **Admin Centers**, select **Azure AD**.

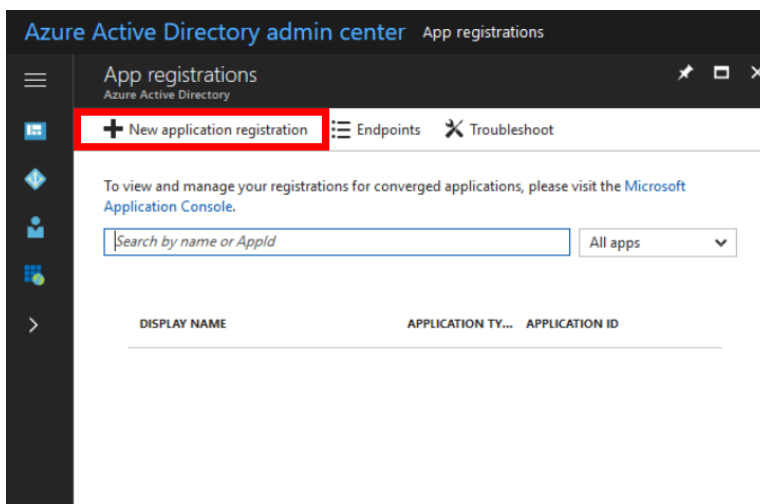


2. Register a new **Application**:

From the **Azure AD Admin Center**, select **More Services**. Then in the filter field, filter by **App registrations**. Then select **App registrations**.

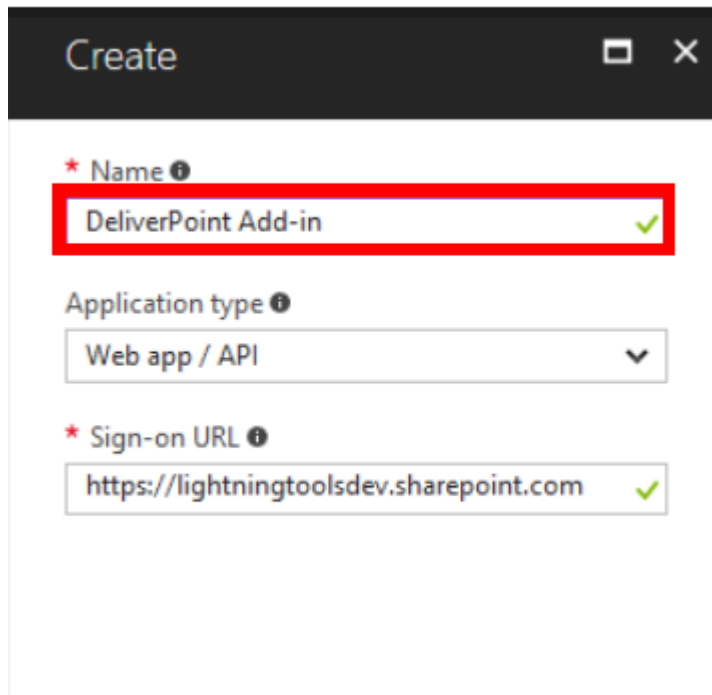


Select **New application registration**.



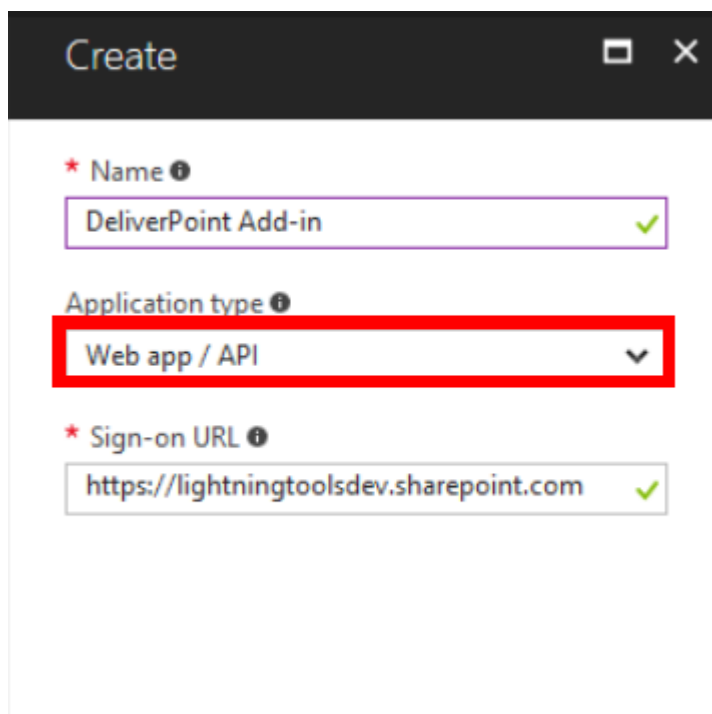
3. Configure your new **Application**

In the **Name** section, call the application **DeliverPoint Add-in**



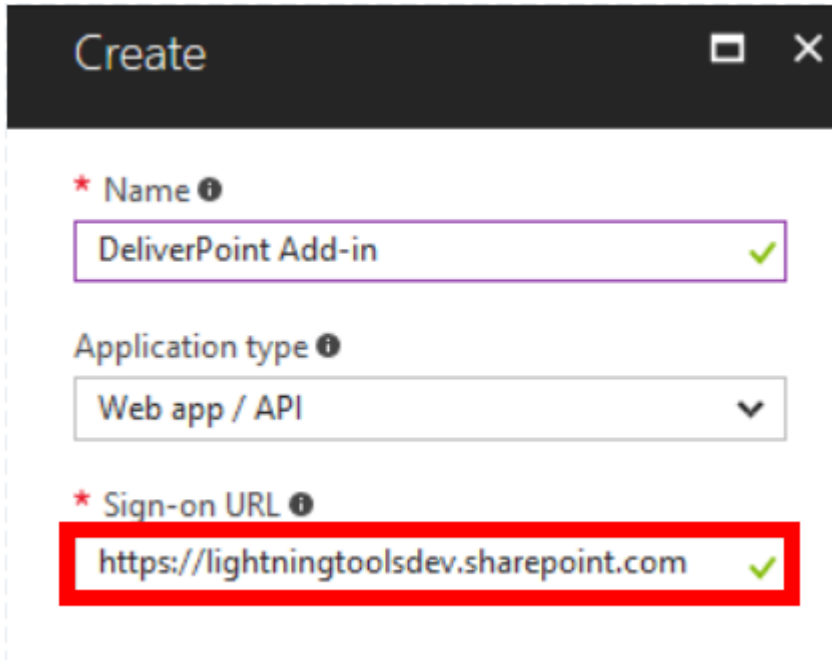
The screenshot shows a 'Create' dialog box with a dark header. The 'Name' field is highlighted with a red border and contains the text 'DeliverPoint Add-in' with a green checkmark. The 'Application type' dropdown is set to 'Web app / API'. The 'Sign-on URL' field contains 'https://lightningtoolsdev.sharepoint.com' with a green checkmark.

In the **Application** type section, select **Web app / API**



The screenshot shows the same 'Create' dialog box. The 'Application type' dropdown is now highlighted with a red border and shows 'Web app / API' with a downward arrow. The 'Name' and 'Sign-on URL' fields remain the same as in the previous screenshot.

In the **Sign-on URL** section, use which ever URL suits you. (It does **NOT** matter which URL you use)
https://example.com would work if you don't know what to use.



Create

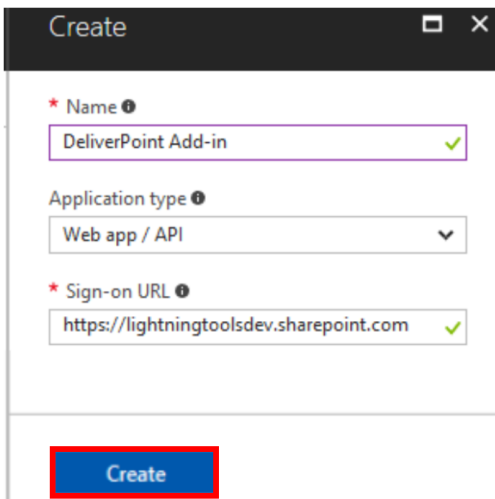
* Name ⓘ
DeliverPoint Add-in ✓

Application type ⓘ
Web app / API ▼

* Sign-on URL ⓘ
https://lightningtoolsdev.sharepoint.com ✓

4. Create your new **Application**

Select **Create**.



Create

* Name ⓘ
DeliverPoint Add-in ✓

Application type ⓘ
Web app / API ▼

* Sign-on URL ⓘ
https://lightningtoolsdev.sharepoint.com ✓

Create

5. Set the **Required permissions**.

Select your new **DeliverPoint Add-in Application**.

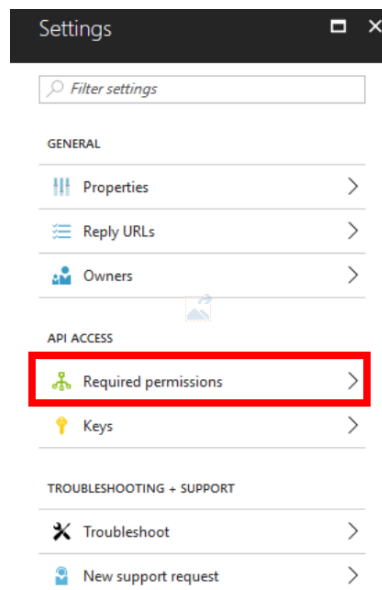
 New application registration  Endpoints  Troubleshoot

To view and manage your registrations for converged applications, please visit the [Microsoft Application Console](#).



All apps ▼

DISPLAY NAME	APPLICATION TY...	APPLICATION ID
 DeliverPoint Add-in	Web app / API	9ff5aad4-9a73-4c85-8f11-ae4...












In **Settings** select **Required permissions**.



In **Required Permissions** select **Windows Azure Active Directory (Microsoft.Azure.ActiveDirectory)**.

Required permissions		
 Add  Grant Permissions		
API	APPLICATION PERMI...	DELEGATED PERMISS...
Windows Azure Active Directory (Microsoft.Azure.Act...	0	1

In the **Application Permissions** select **Read directory data**.

Enable Access	
Microsoft.Azure.ActiveDirectory	
 Save  Delete	
 You are adding permission(s) that require an admin to consent, users will not be able to use the application until an admin grants permissions to the application.	
<input type="checkbox"/> APPLICATION PERMISSIONS	<input type="checkbox"/> REQUIRES ADMIN
<input checked="" type="checkbox"/> Read directory data	 Yes
Read and write domains	 Yes
Read and write directory data	 Yes
Read and write devices	 Yes
Read all hidden memberships	 Yes
Manage apps that this app creates or owns	 Yes
Read and write all applications	 Yes
Read and write domains	 Yes

In **Delegated Permissions** select **Access the directory as the signed-in user**, **Read directory data** and **Sign in and read user profile**.

DELEGATED PERMISSIONS		REQUIRES ADMIN
<input checked="" type="checkbox"/>	Access the directory as the signed-in user	No
<input checked="" type="checkbox"/>	Read directory data	Yes
	Read and write directory data	Yes
	Read and write all groups	Yes
	Read all groups	Yes
	Read all users' full profiles	Yes
	Read all users' basic profiles	No
<input checked="" type="checkbox"/>	Sign in and read user profile	No
	Read hidden memberships	Yes

6. Create your **Application Key**.

Select your new **DeliverPoint Add-in Application**.

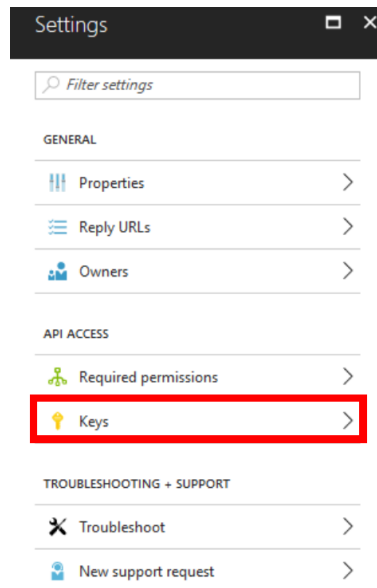
[+ New application registration](#)
[Endpoints](#)
[Troubleshoot](#)

To view and manage your registrations for converged applications, please visit the [Microsoft Application Console](#).

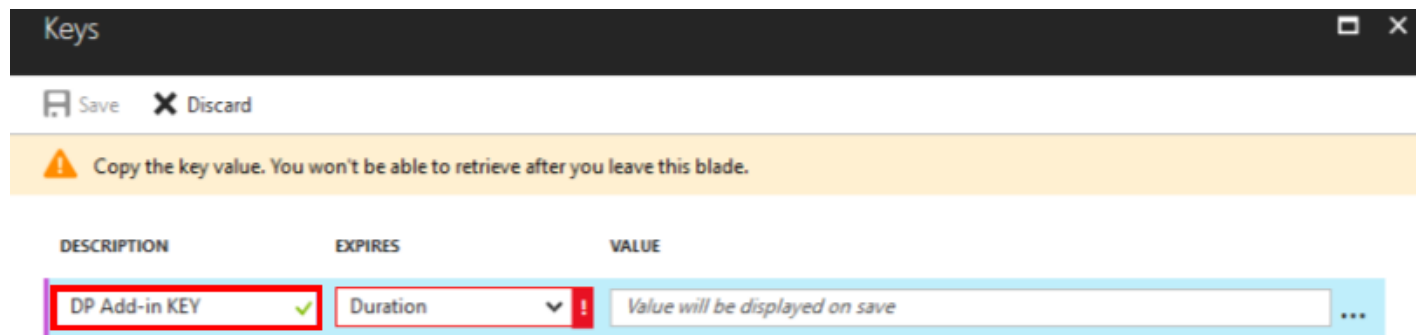
All apps
▼

DISPLAY NAME	APPLICATION TY...	APPLICATION ID
DA DeliverPoint Add-in	Web app / API	9ff5aad4-9a73-4c85-8f11-ae4...

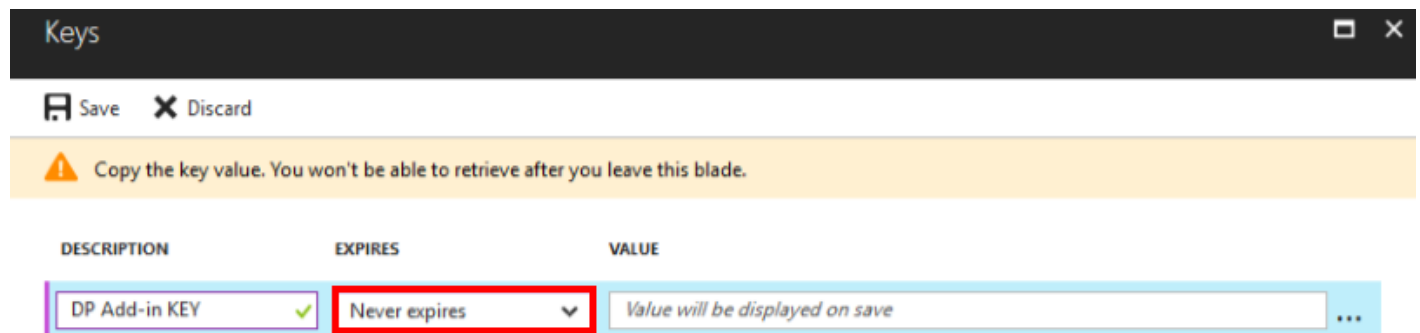
In **Settings** select **Keys**.



In the **Description** box, give your key a name.

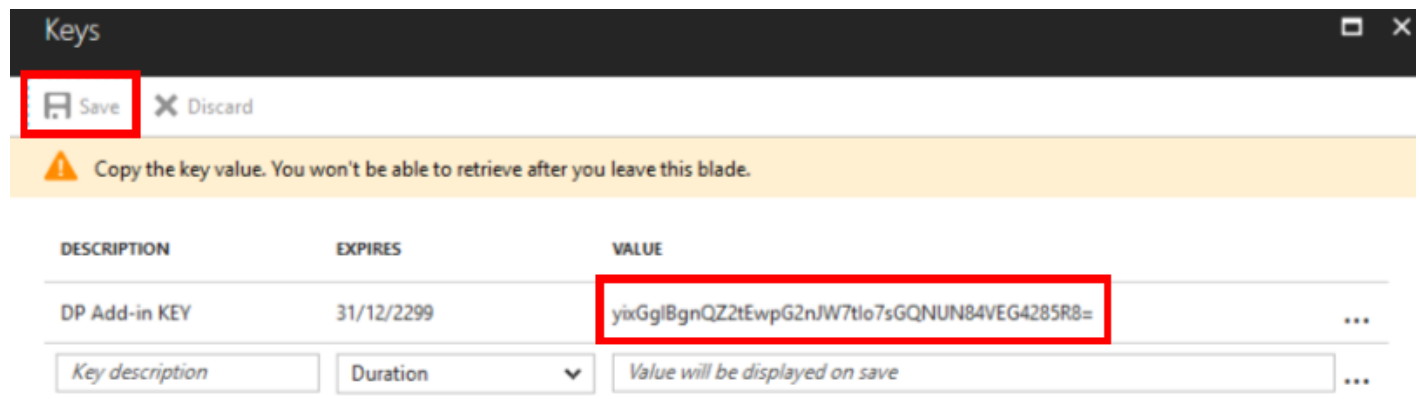


In the **Expires** box, select **Never expires**.



Select **Save**, then copy the **Value** and make sure you make a copy of this, as you'll need it to configure the DeliverPoint Add-in **Application Key**.

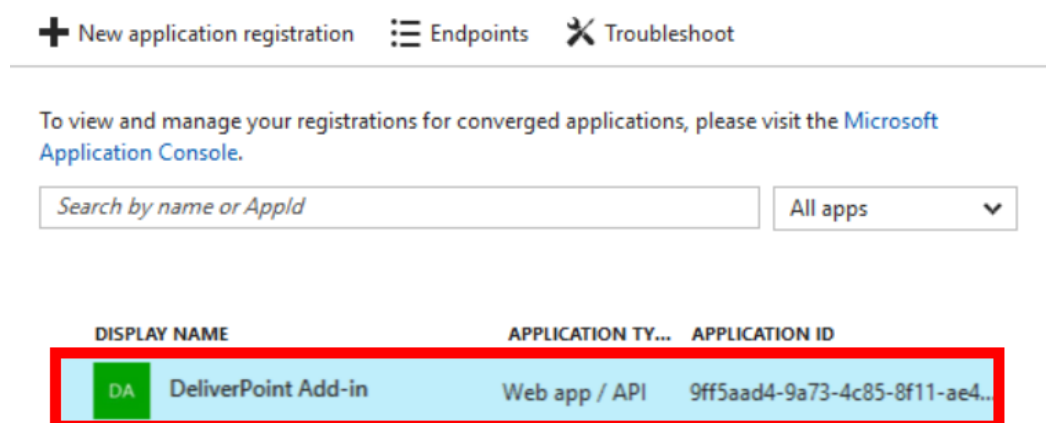
Tip: You will not be able to retrieve the key, once you leave the page. If you do not save the key, you'll need to generate a new one.



DESCRIPTION	EXPIRES	VALUE
DP Add-in KEY	31/12/2299	yixGglBgnQQZ2tEwpG2nJW7tlo7sGQNUN84VEG4285R8=

7. Copy the **Application ID**

Select your new **DeliverPoint Add-in Application**.



DISPLAY NAME	APPLICATION TY...	APPLICATION ID
DA DeliverPoint Add-in	Web app / API	9ff5aad4-9a73-4c85-8f11-ae4...

Copy down the **Application ID** as you'll need this to configure the DeliverPoint Add-in

DeliverPoint Add-in

Registered app

Settings

Manifest

Delete

Essentials ^

Display name	Application ID
DeliverPoint Add-in	9ff5aad4-9a73-4c85-8f11-ae4d68253fc4
Application type	Object ID
Web app / API	c981f7d2-1b65-45a9-8227-e8dcdbd50f087
Home page	Managed application in local directory
https://lightningtoolsdev.sharepoint.com	DeliverPoint Add-in

[<< Upload Add-In to App Catalog](#)

[Adding the Add-In to a Site >>](#)

References


- [Understanding Office 365 identity and Azure Active Directory](#)
- [Azure Active Directory editions](#)
- [Administering your Azure AD directory](#)

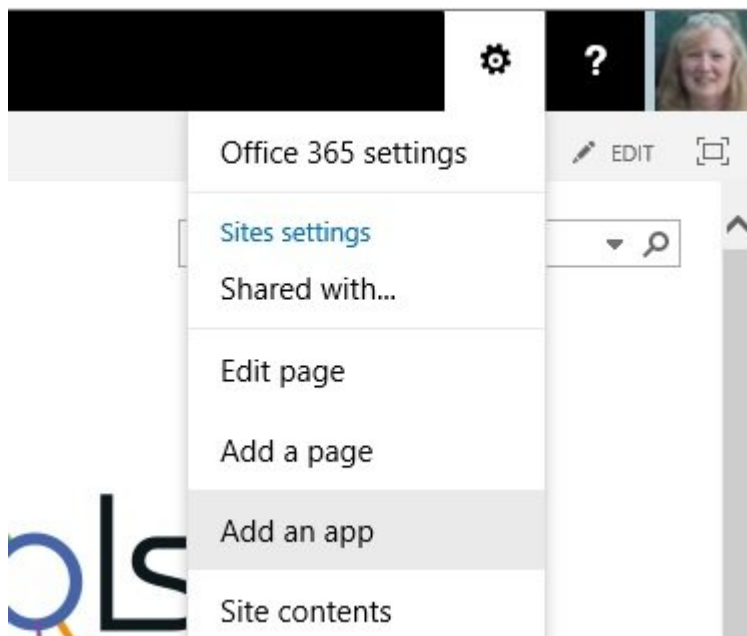
Adding the Add-In to a Site

To use the DeliverPoint Add-In, you first need to add the DeliverPoint Add-In to a site in the site collection where you want to create a discover permissions report. There are many ways of [adding an Add-In to a site](#). The steps in this section, assume that the *DeliverPoint* Add-In appears under *From Your Organization* in the *App Catalog*. To add the *DeliverPoint* Add-In to the *App Catalog*, use the steps documented in the [Installation of Add-In](#) section of this online manual.

To add the [DeliverPoint Add-In](#) to a site, use the following steps. :

! You need to be mapped to the Full Control [permission level](#) to complete the following steps. If you are a Site Owner, then you will be mapped to this permission level.

1. Navigate to the site where you wish to use the DeliverPoint Add-In.
2. Click **Settings**  in the top right corner of the team site, and then click **Add an app**.



3. On the **Your Apps** page, under **Apps you can add**, click **DeliverPoint**.

Tip: In your organization you may find the *DeliverPoint* add-in below **Noteworthy**. If your organization

has many apps, to quickly find the app, type **DeliverPoint** in the **Find an app** search box.

4. On the **Do you trust DeliverPoint** dialog, click **Trust It**.

The *Site Contents* page is displayed, and the app will begin to install. It will first appear grayed during the installation, and then when the installation is complete you will see the DeliverPoint add-in.

You can now start to use the Add-In, as described in the in the [Using the Add-in](#) section of this online manual.

[<< Create Windows Azure Application](#)

[Configure DeliverPoint Add-In >>](#)

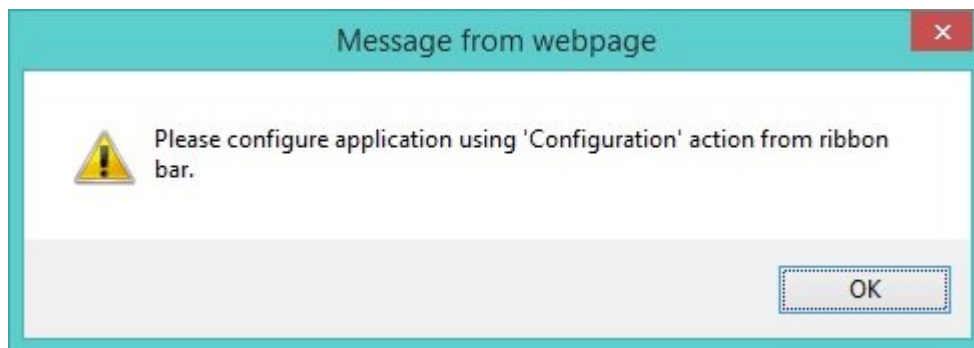
Related Office.com documentation

- [Add an app to a site →](#)
- [Monitor apps for a site →](#)
- [Remove an app from a site →](#)
- [Permissions in Office 365 →](#)
- [Introduction: Control user access with permissions →](#)
- [Understanding permission levels →](#)

Configure DeliverPoint Add-In

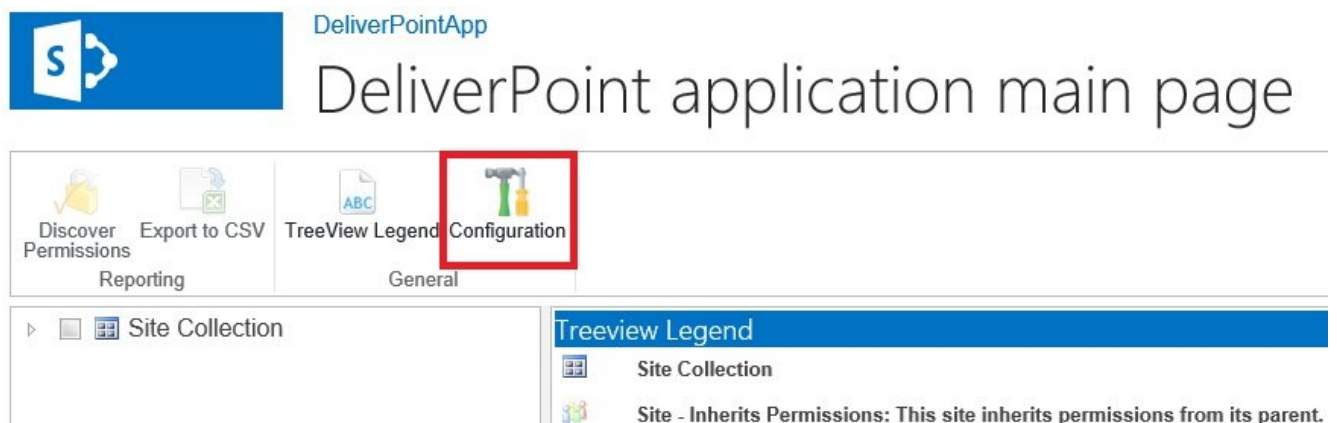
Before you can use the DeliverPoint Add-In, it must be configured with the Office 365 tenant domain, and the client id and secret key that was created when the [Windows Azure application was created](#). Once you have those three pieces of information, complete the following steps:

1. Navigate to a site where you have added the DeliverPoint Add-In.
2. From the Quick Launch or the site contents page, click **DeliverPoint**.
3. If a dialog box is displayed, stating to *Please configure the application, using the 'Configuration' command on the Ribbon*, click **OK**.



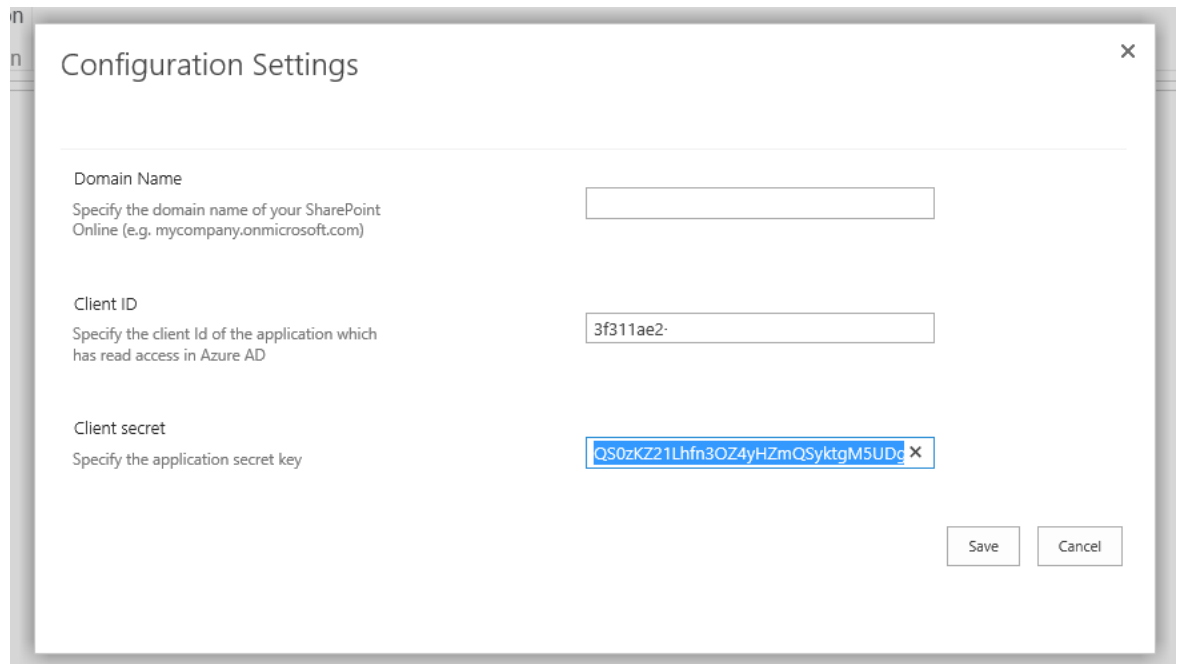
The DeliverPoint application main page is displayed.

4. On the Ribbon, click **Configuration** in the **General** group.



5. In the **Configuration Settings** dialog:

- In the Domain Name text box, type the domain name of your Office 365 tenant, for example, lightning365.onmicrosoft.com
- In the **Client ID** text box, type the Client ID of the Azure application you saved previously.
- In the **Client secret** text box, type the Key of the Azure application you previously saved.



The image shows a 'Configuration Settings' dialog box with three input fields. The first field is 'Domain Name' with a placeholder 'Specify the domain name of your SharePoint Online (e.g. mycompany.onmicrosoft.com)'. The second field is 'Client ID' with a placeholder 'Specify the client Id of the application which has read access in Azure AD' and contains the value '3f311ae2'. The third field is 'Client secret' with a placeholder 'Specify the application secret key' and contains the value 'QS0zKZ21Lhfn3OZ4yHZmQSyktgM5UDg'. There are 'Save' and 'Cancel' buttons at the bottom right.

Field	Value
Domain Name	
Client ID	3f311ae2
Client secret	QS0zKZ21Lhfn3OZ4yHZmQSyktgM5UDg


- Click **Save**.

[<< Adding the Add-In to a Site](#)

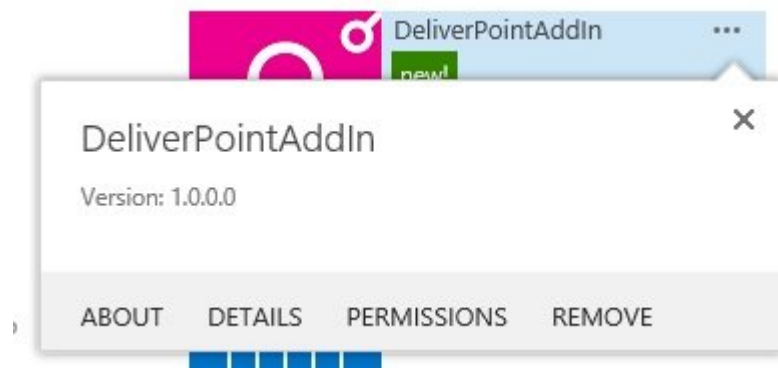
[How to tell the version of the Add-In >>](#)

How to tell the version of the Add-In

To find the version of the DeliverPoint Add-In complete the following:

1. Navigate to a site where you have [added the DeliverPoint Add-In](#).
2. Either on the Quick Launch click **Site Contents** or from the **Setting**  menu, click **Site Contents**.
3. Point to the tile for the DeliverPoint Add-In, and click the ellipse (...) next to the add-in name.

A callout displays which contains version information.



The DeliverPoint callout provides the following links.

- **About.** Use to display the DeliverPoint page on the SharePoint Store.
- **Details.** Use to display the **App Details** page, which allows a site owner to monitor information about the Add-In, for example, you can view information about how often the Add-In has been launched and how many errors the Add-In has had. For more information of this option, see the Microsoft Office support page, [Monitor apps for a Site](#).
- **Permissions.** Use to display the permissions of the DeliverPoint Add-In.
- [Remove.](#) Use this link if you no longer need the DeliverPoint Add-In on your site.

Note: To [remove an Add-In](#), you must have Full Control permissions for the SharePoint site. If you are a Site Owner, you are mapped to this permission level.


[<< Configure DeliverPoint Add-In](#)

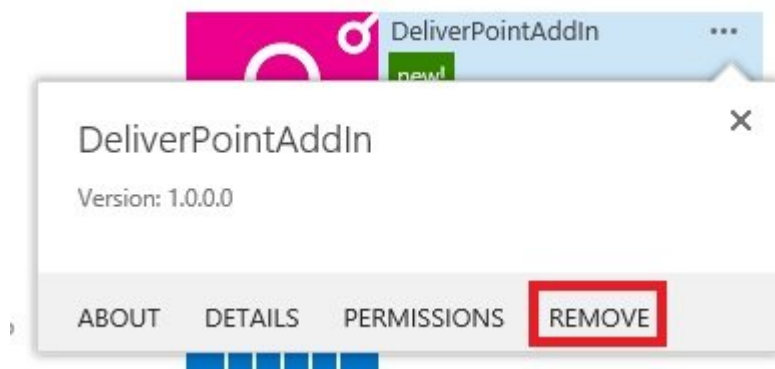
[Removing the Add-In from a Site >>](#)

Removing the Add-In from a Site

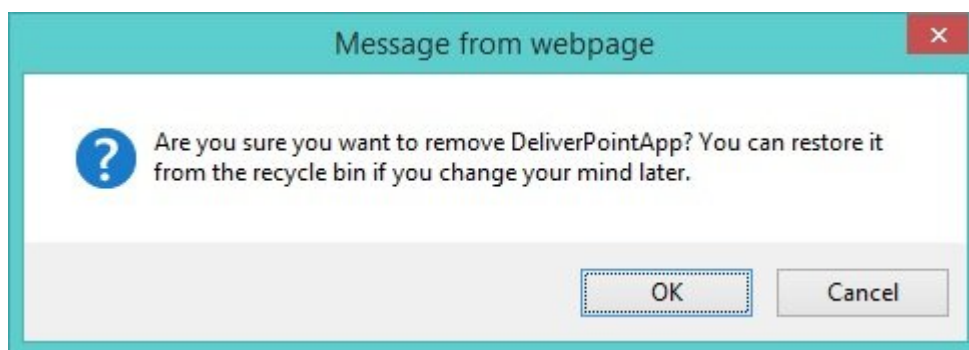
To remove the [DeliverPoint Add-In](#) from a site, use the following steps. :

! You need to be mapped to the Full Control permission level to complete the following steps. If you are a Site Owner, then you will be mapped to this permission level.

1. Navigate to the site where you wish to remove the DeliverPoint Add-In.
2. Either, on the Quick Launch, click **Site Contents** or from the **Settings**  menu click **Site Content**.
3. On the *Site Contents* page, point to the tile for the DeliverPoint Add-In, click the ellipse (...) next to the Add-In name and then click **Remove**.



4. Click **OK** to close the dialog box asking you if you are sure you want to remove the Add-In.



The Add-In is removed from the site, and placed in the recycle bin.

Note: If you try to add the Add-In once it is removed, you may see an error that you may need to delete the Add-In from the site and the site collection recycle bin to install the Add-In. Instructions on how to delete an Add-In from the recycle bins are documented next on this page.



Although you can restore the Add-In from the recycle bin, permissions to the Add-In will not be configured correctly and no one will be allowed access to the Add-In. Therefore if you need to use the Add-In again on a site, you should always delete the Add-In from the both the end user's and second-stage recycle bins, if it still exists there, and then [add the DeliverPoint Add-In](#).

To delete the Add-In from the recycle bin, use the following steps:

1. Navigate to the site where you removed the DeliverPoint Add-In.
2. Either, on the Quick Launch, click **Recycle Bin** or from the **Site Contents** page click **Recycle Bin**.
3. On the *Recycle Bin* page, select the check box to the left of the Add-In, and then click **Delete Selection**.

Note: The Add-In, unless deleted from the recycle bin, will remain in the end user's recycle bin for 30 days.

4. Click **OK** to close the dialog box, *Are you sure you want to remove "DeliverPoint from the end user's Recycle Bin"*.
5. At the bottom of the *Recycle Bin* page, click **second-stage recycle bin**.
6. On the *Second-Stage Recycle Bin* page, select the check box to the left of the Add-In, and then click **Delete Selection**.
7. Click **OK**, to close the dialog box, *Are you sure you want to permanently delete this item*.

Note: The Add-In, once deleted from the end user's recycle bin, remains in the second-stage recycle bin for 93 days, unless the previous step is completed.

References

- [Manage the Recycle Bin of a SharePoint Online site collection](#)
- [Empty the recycle bin or restore your files](#)

[<< How to tell the version of the Add-In](#)

[Using the Add-in Professional >>](#)

Using the Add-in Professional

The [DeliverPoint SharePoint Online Add-In for Office 365 Professional](#) provides reporting and management of permissions within your Microsoft® SharePoint® Online Office 365™ tenant.

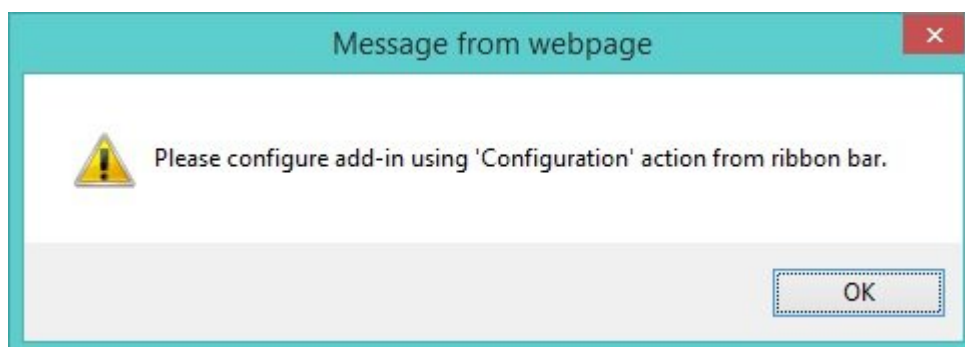
* Users can only use the DeliverPoint [Discover Permissions](#) action if they have the SPBasePermission Enumerate permission, that is, only users who have access to view permissions in SharePoint can access this DeliverPoint action. For example, users who are mapped to a permission level that includes the Manage Permissions right, such as, Full Control, will be able to use this action.

You can use the DeliverPoint Add-In to manage permissions at the [top level site of a site collection](#), [site](#), [list/library](#) and [list item/file](#) levels.

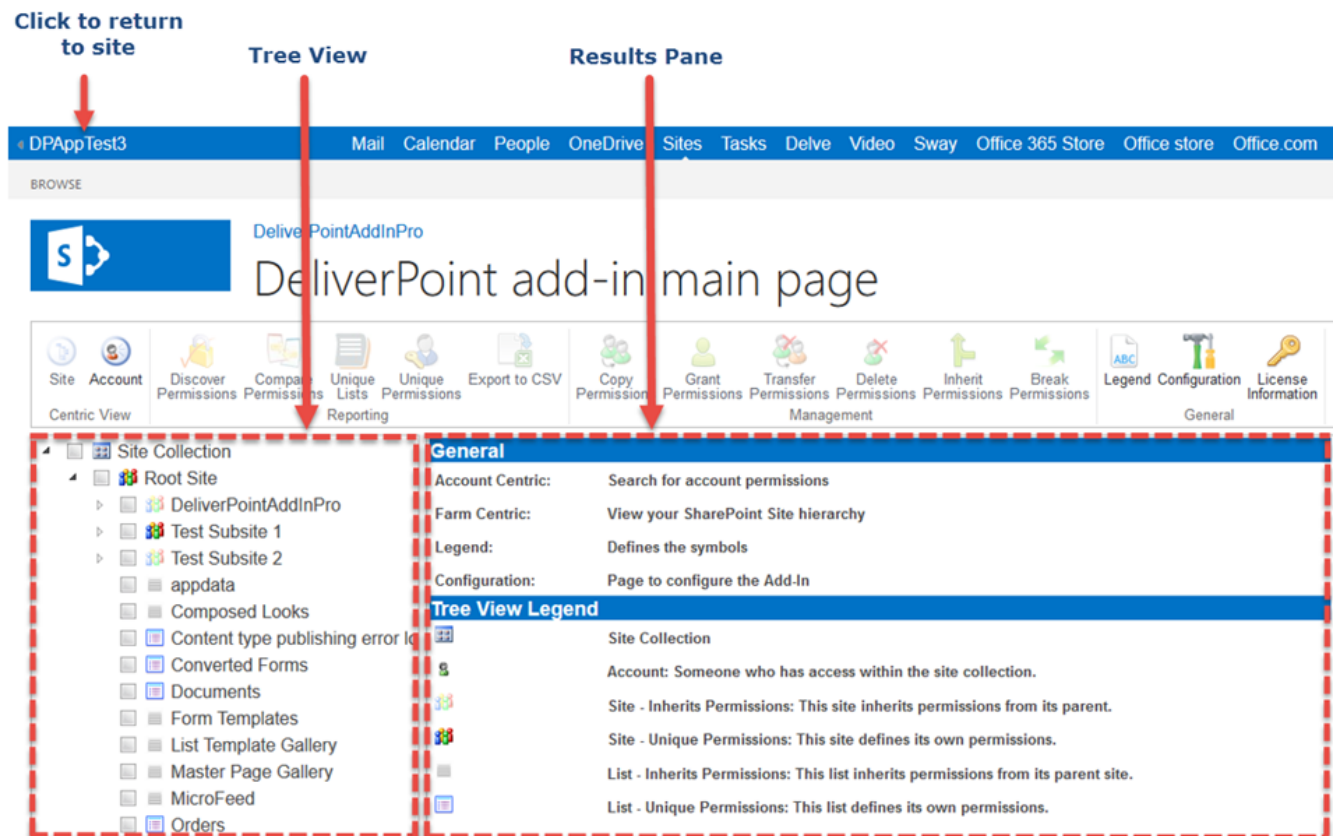
Site, List, and Library Permission Management

To use the DeliverPoint Add-In at the site collection, site, list or library levels, use the DeliverPoint Add-In Main Page. To navigate to the DeliverPoint Add-In Main Page, complete the following steps:

1. Navigate to a site where you have added the DeliverPoint Add-In Pro.
2. From the Quick Launch or the site contents page, click **DeliverPoint Add-In Pro**.
3. If a dialog box is displayed, stating to please configure the application, using the Configure action on the Ribbon, click **OK**, and then complete the steps described in the [Configuring the DeliverPoint Add-in](#) section.



The DeliverPoint Add-In main page is displayed.



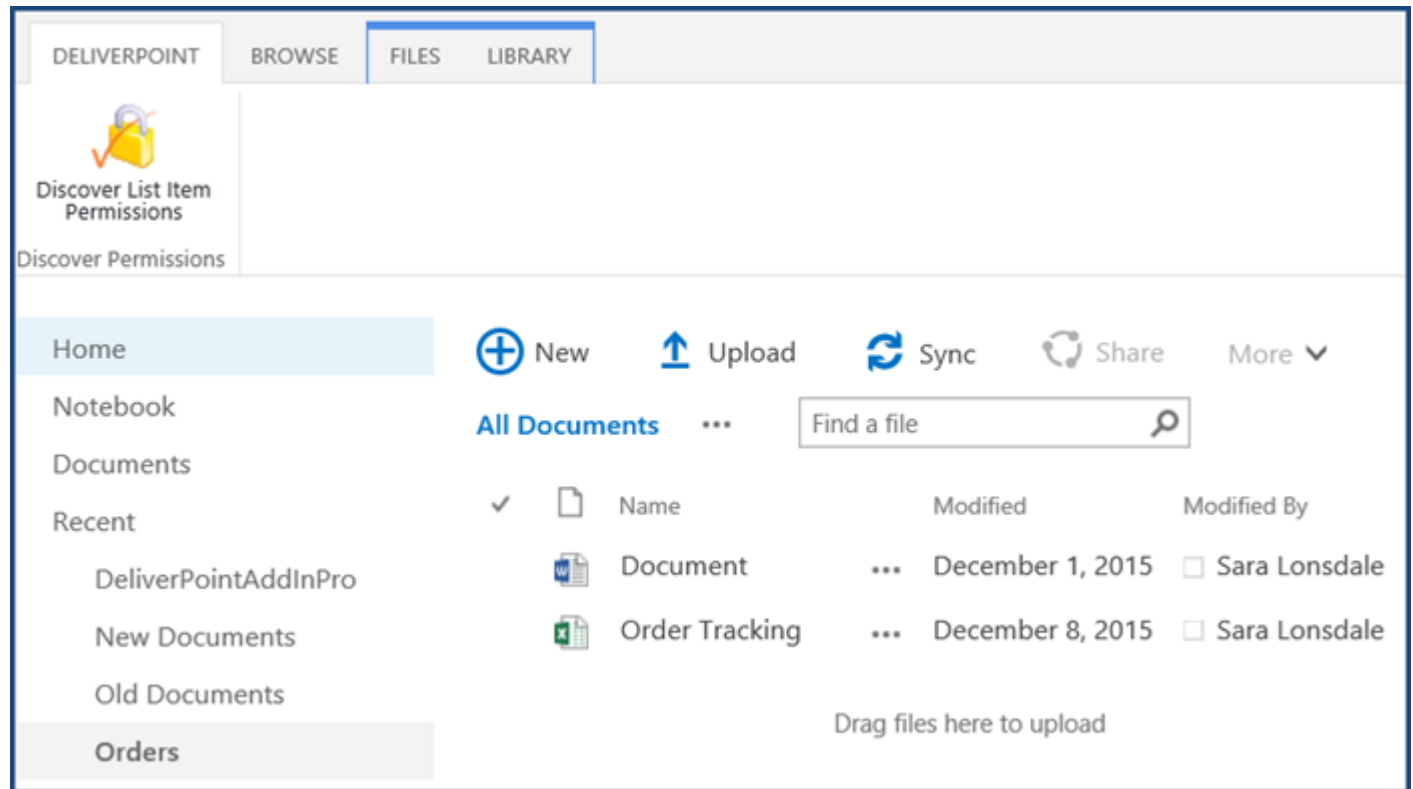
The DeliverPoint Add-In main page consists of:

- **Ribbon.** This contains the commands to complete the following actions:
 - **Centric View**
 - **Site.** Allows the user to set the scope for reporting by selecting one or more objects in the site structure, which is displayed via the Tree View.
 - **Account.** Allows the user to search for a user account or security group, on which a report can be run against. This view is also used if the user wants to run a Unique Permissions report on a specific user account or SharePoint/security group.
 - **Reporting**
 - **Discover Permissions.** Allows the user to find out who has access to a given object and how that access is given.
 - **Compare Permissions.** Allows the user to compare permissions between more than one object, such as between two subsites.
 - **Unique Lists.** Allows the user to report any lists which have unique permissions, or in other words, lists which have had their permissions broken from the parent site.

- **Unique Permissions.** Via the Account Centric View, the user can run this report to find the locations where a specific user account or security group has been given explicit permissions to a site collection, site, list/library, folder or list item. In other words, where a user or group does not have its permissions inherited from the parent object.
- **Export to CSV.** Allows you to export the results to a comma-separated values (CSV) file, which you could then open in a program, such as Microsoft® Excel, to analyse the data.
- **Management**
 - **Copy Permissions.** Allows the user to copy permissions from one object (source) to another (target). Copying amends permissions on the target object, and does not affect the existing permissions.
 - **Grant Permissions.** Allows the user to grant permissions on one or more selected objects to a user account and/or SharePoint/security group, or combination of users and/or groups.
 - **Transfer Permissions.** Allows the user to select a scope, copy the permission set of an account (source) within that scope to other account(s) (target), and then the source account is deleted within the selected scope. This operation is a combination of the Copy Permissions and Delete Permissions commands.
 - **Delete Permissions.** Deletes an account's permissions on an object.
 - **Inherit Permissions.** Allows the user to re-inherit the permissions of the parent object. This action is applied to objects that have unique permissions.
 - **Break Permissions.** Allows the user to break the inheritance of an object from its parent, thus giving the user the ability to modify the permissions of that object. This results in an object having unique permissions.
- **Tree View**
 - **Tree View Legend.** Displays a legend of the icons used in the tree view area.
 - **Configuration.** Use to configure the DeliverPoint Add-In.
 - **License Information.** Displays product licence details.
 - **Online Documentation.** Link to this documentation.
- **Tree View pane.** The tree view area, displays the site collection, the sites within the site collection, and the lists and libraries within each site that you have permissions to view. You will use the check box to the left of each SharePoint object displayed to identify which object to complete the permission management task.
- **Results pane.** As you complete different DeliverPoint tasks, the results pane is used to display the results of those tasks. When you first display the DeliverPoint Add-In Main Page, the result pane displays the legend of the icons that appear in the tree view.
- **Selected Scope pane.** This pane is displayed at bottom of the DeliverPoint Add-In Main Page and displays the SharePoint object(s) selected in the tree view pane.







List Item and File Permission Management

On sites where you have added the DeliverPoint Add-In, you can complete DeliverPoint Add-In permission management tasks on list items and files. Lists and libraries in sites where the DeliverPoint Add-In has been added will display on the DeliverPoint Ribbon tab.



[<< Removing the Add-In from a Site](#)
[Add-In ProTree View Legend >>](#)

Add-In ProTree View Legend

Icon	Description
	Site collection
	Account: Someone who has access within the site collection.
	Site that inherits permissions from parent site. When you create a subsite, the default is always to inherit its permissions from the parent site.
	Site with unique permissions, that is, the site does not inherit its permissions from a parent site. The site defines its own permissions. The top-level site of a site collection is always a site with unique permissions.
	List that inherits permissions from the parent site. When you create a list or library, the default is always to inherit its permissions from the parent site.
	List with unique permissions, that is, the list or library does not inherit its permission from a parent site. The list or library defines its own permissions.

[<< Using the Add-in Professional](#)

[Discovering Permissions >>](#)

Discovering Permissions

Discover Permissions allows the user to find out who has access to a given object and how that access is given.

- * Users can only use the DeliverPoint **Discover Permissions** action if they have the SPBasePermission Enumerate permission, that is, only users who have access to view permissions in SharePoint can access this DeliverPoint action. For example, users who are mapped to a permission level that includes the Manage Permissions right, such as, Full Control, will be able to use this action.

There are three forms of the *Discover Permissions* DeliverPoint action:

- [Discover Site Permissions](#)
- [Discover List Permissions](#)
- [Discover Folder/Item/File Permissions](#)

All three forms of this DeliverPoint action uses the Discover Permissions with DeliverPoint results page, which you can use to filter the results. The Discover Permissions with DeliverPoint results page and how to filter the results are explained in the next sections.

[<< Add-In ProTree View Legend](#)

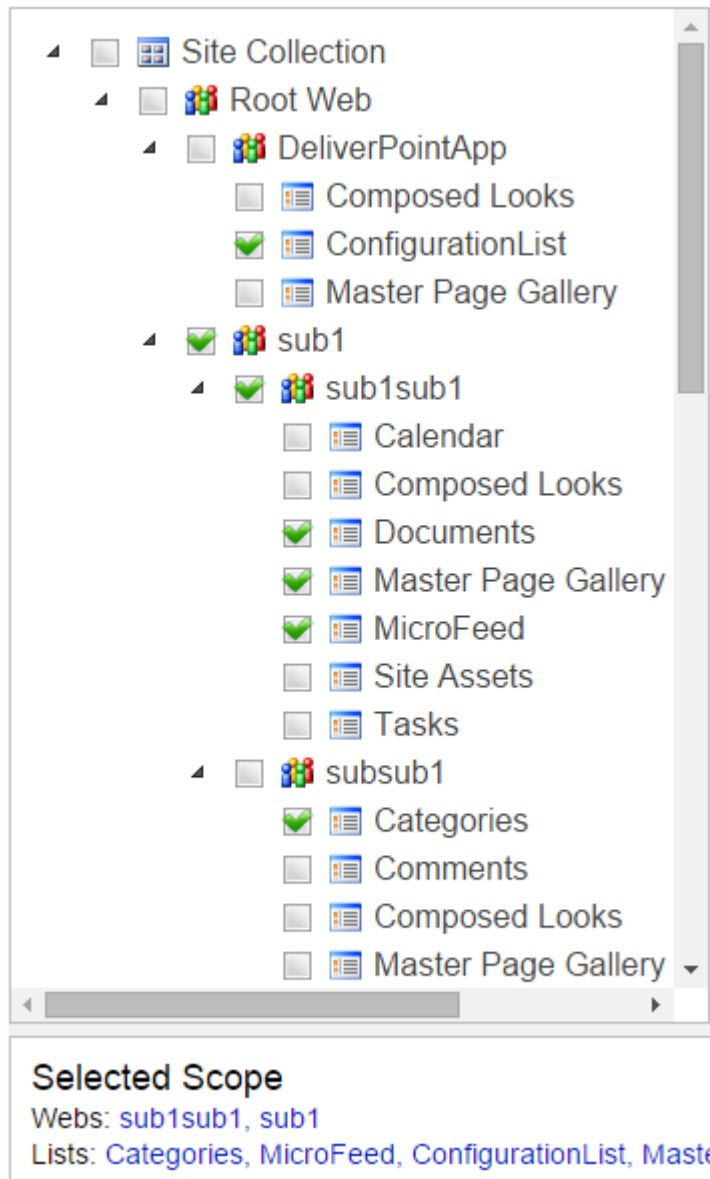
[Discover Site and List Permissions >>](#)

Discover Site and List Permissions

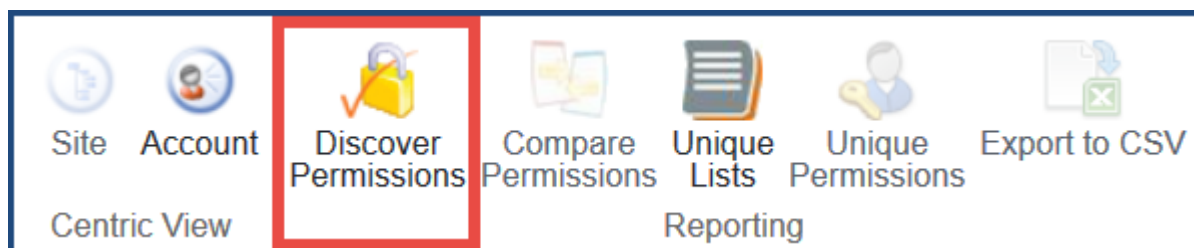
The steps for Discovering Site and List permissions is the same.

To Discover Site or List permissions:

1. Display the **DeliverPoint Add-In Main Page**.
2. In the left hand navigation, expand the tree view and select the check boxes to the left of the required SharePoint object(s). **Note:** *The order you select the objects affects the order that the objects are displayed in the report. Subsites, lists, and libraries will only appear in the report if selected. By selecting just the top level site in a site collection, only the configuration at the site level are reported.*



3. On the Ribbon, click **Discover Permissions** in the **Reporting** group.



The *Discover Permissions report* is displayed in the results pane of the *DeliverPoint Add-In Main Page*.

Scope	User	Permission	Via
DPAppTest3	System Account	Full Control	DPAppTest3 Owners
DPAppTest3	Brett Lonsdale	Read	DPAppTest3 Visitors
DPAppTest3	Judy Carthy	Read	DPAppTest3 Visitors
DPAppTest3	Jarrad Carter	Read	DPAppTest3 Visitors
DPAppTest3	Ryan Newman	Read	DPAppTest3 Visitors
DPAppTest3	Oliver Pick	Read	DPAppTest3 Visitors
DPAppTest3	David Hartley	Read	DPAppTest3 Visitors
DPAppTest3	Ara Arakelyan	Edit	DPAppTest3 Members
DPAppTest3	Ara Arakelyan	Limited Access	DPAppTest3 Members
DPAppTest3	Brett Lonsdale	Edit	DPAppTest3 Members
DPAppTest3	Brett Lonsdale	Limited Access	DPAppTest3 Members
DPAppTest3	Karen Khumaryan	Edit	DPAppTest3 Members
DPAppTest3	Karen Khumaryan	Limited Access	DPAppTest3 Members
DPAppTest3	Sandy Ussia	Edit	DPAppTest3 Members
DPAppTest3	Sandy Ussia	Limited Access	DPAppTest3 Members
DPAppTest3	Zorayr Zakaryan	Edit	DPAppTest3 Members
DPAppTest3	Zorayr Zakaryan	Limited Access	DPAppTest3 Members

Selected Scope
 Sites: Root Site
 Lists: Orders

In the bottom pane, the SharePoint objects that were selected to create the report are listed, for example, in the above screen shot the top level site of the site collection (Root Site) and the list *Orders* were selected.

- To return to the home page of your SharePoint site, click the link in the top left corner.

DPAppTest3

BROWSE

DeliverPointAddInPro

DeliverPoint add-in main page

Site Account Discover Permissions Compare Permissions Unique Lists Unique Permissions Export to CSV Clone Permissions Grant Permissions Transfer Permissions

CentricView Reporting Management

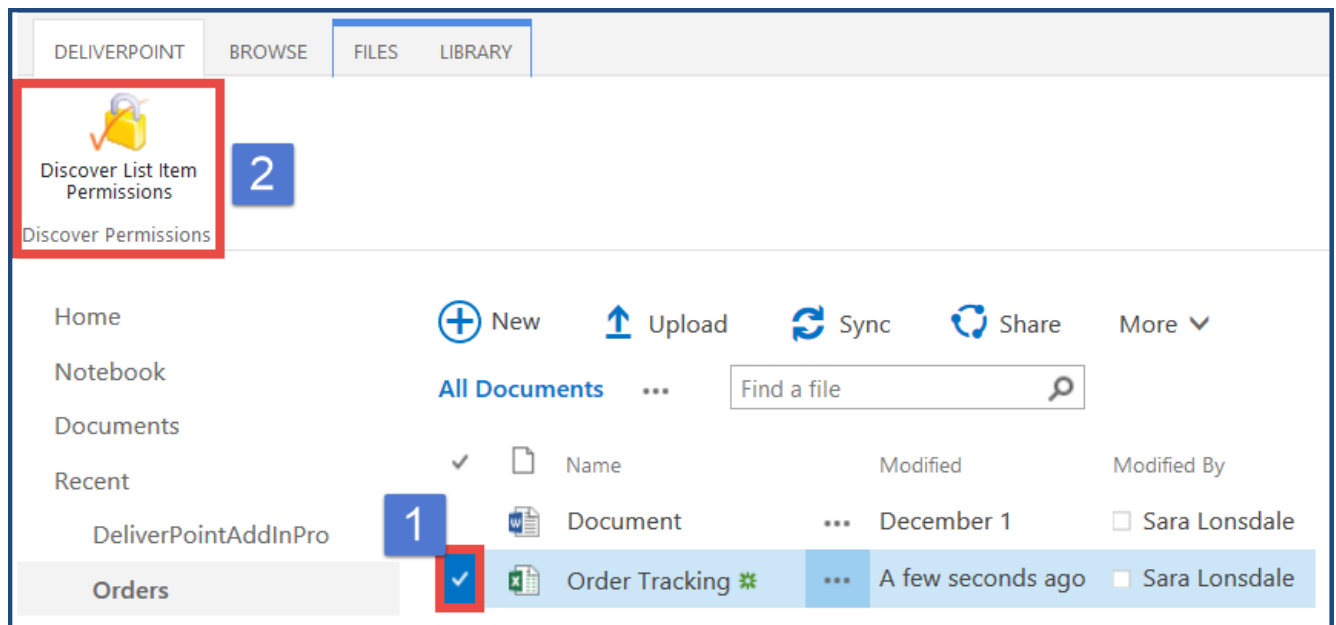
[<< Discovering Permissions](#)

[Discover Folder, Item, or File Permissions >>](#)

Discover Folder, Item, or File Permissions

To use the [Discover Permissions](#) action on a folder, list item, or file, complete the following steps:

1. Navigate to the list where you want to use the DeliverPoint **Discover Permissions** command.
2. Click to the left of one or more folders, list items, or files, and then on the DeliverPoint Ribbon tab, click **Discover List Item Permissions**.



The *Discover Permissions with DeliverPoint Add-In Main Page* is displayed.

[<< Discover Site and List Permissions](#)

[Discover Permissions Results >>](#)

Discover Permissions Results

The **Discover Permissions** results are batched as (maximum) 50 results per page. At the bottom of the page there are page numbers you can use to display each set of 50 results.

Site

Account

Discover Permissions

Compare Permissions

Unique Lists

Unique Permissions

Export to CSV

Copy Permissions

Grant Permissions

Transfer Permissions

Delete Permissions

Inherit Permissions

Break Permissions

Centric View

Site Collection

Root Site

DeliverPointAddInPro

Test Subsite 1

Test Subsite 2

appdata

Composed Looks

Content type publishing error lo

Converted Forms

Documents

Form Templates

List Template Gallery

Master Page Gallery

MicroFeed

Orders

Site permissions

Scope

User

Permission

Permissioned Via

DPAppTest3

System Account

Full Control

DPAppTest3 Owners

DPAppTest3

Brett Lonsdale

Read

DPAppTest3 Visitors

DPAppTest3

Brett Lonsdale

Limited Access

DPAppTest3 Visitors

DPAppTest3

Judy Carthy

Read

DPAppTest3 Visitors

DPAppTest3

Judy Carthy

Limited Access

DPAppTest3 Visitors

DPAppTest3

Jarrad Carter

Read

DPAppTest3 Visitors

DPAppTest3

Jarrad Carter

Limited Access

DPAppTest3 Visitors

DPAppTest3

Ryan Newman

Read

DPAppTest3 Visitors

DPAppTest3

Ryan Newman

Limited Access

DPAppTest3 Visitors


The page contains the following columns:

- **Scope.** When the hyperlink is clicked the home (default) page of the site/list or the property page of the list item/file is displayed.
- **User.** The account's Display Name.
- **Permission.** The permission level(s) that is mapped to the account on the object.
- **Permissioned Via.** Lists graphically how the user has been given access to the object. To expand SharePoint Groups, click the plus sign (+) to the left of the group name.

Sorting the Results

You can sort the results using the column headings **Scope**, **User**, **Permission**, and **Permissioned Via**. Sorting is completed against all the results returned, that is, sorting is not limited to the 50 results displayed on a specific page when there are more than 50 results are returned.

Filtering the results

The Filter icon  displayed to the right of each column heading can be used to refine the results returned. See the next section for more information on how to filter the results of the discover permission action.


Exporting the results

To export the results, click **Export to CSV** on the Ribbon in the **Reporting** group. The Microsoft® Excel spreadsheet file name is of the format, *ExportDiscoveredPermissions_YYYY-MM-DDXXX.csv*, where XXX is the timestamp unique for each file. All results are exported, that is, the results exported are not limited to the results displayed on a specific page when more than 20 results returned from the [Discover Permissions](#) command.




[<< Discover Folder, Item, or File Permissions](#)


[Refining Discover Permissions Results >>](#)

Refining Discover Permissions Results




The [Discover Permission results](#) can be customized using the Filter icon  to the right of the column headings.

Column Heading Filtering

Use the *Filter* icon  displayed to the right of each column heading to filter the [Discover Permissions results](#) by **Scope**, **User**, **Permission**, or **Permissioned Via**. When a filter is configured for a column heading then the *Remove Filter* icon  is displayed to the right of the filter icon .

When you click the *Filter* icon  a dialog box opens that allows you to configure one or more filter criteria. By default the *Filter Configuration* dialog contains three drop down lists for you to configure one filter criteria.

Each filter criteria consists of three input boxes:

1. **And/Or** box. This drop-down is available only when an additional criteria is added using the  icon.
 - a. To add another criteria, click the green plus icon  :
 - i. Select **And** to create a filter where the data must match the criteria in all filter criteria.
 - ii. Select **Or** to create a filter where the data must match the criteria in only one filter criteria.
 - b. Each criteria can be removed from the filter by clicking the remove filter icon .
2. The **Operation** box. This drop-down contains operators to use against the results. The following operators available are: **Equals**, **Does not equal**, **Begins With**, **Contains**, **Like**, **Not Like**, **Match**, **Not Match**, **Is Null**, **Is not Null**.

Filter configuration for 'User'

Add new filter condition

And

Save

- Equals
- Does not equal
- Begins With
- Contains
- Like
- Not Like
- Match
- Not Match
- Is Null
- Is Not Null

st3 Lonsdale
st3 Lonsdale
st3 Carthy

3. The **Value** box. Select or type the criteria that you want to include. For instance, when you select the *Permissions* column heading filter, the values listed in the *Value* drop-down will be the permission levels displayed in the results page. When you select the *Permissioned Via* column heading filter, the values listed in the *Value* box are the Users, Active Directory groups, and SharePoint groups that are displayed on the results page.

Filter configuration for 'Permissioned Via'

Add new filter condition

And

Save Cancel

DPAppTest3 Owners

* **Example:** If when filtering on the *Permissioned Via* column you want to show all results that have users in any Active Directory or SharePoint group with 'Manager' in the name, you could select 'Contains' from the *Operator* field and then type 'Manager' in the *Value* field.

This would display all users in the report who are members of one or more groups containing the word 'Manager'.


Once the filter is configured click **Save**.









Filter configuration for 'User'

Add new filter condition

And
Contains
Brett

Save
Cancel

To edit an existing filter, click the *Filter* icon again. To remove a filter, click the *Remove Filter* icon .

Site permissions			
Scope ▼	User ▼ 	Permission ▼	Permissioned Via ▼
DAppTest3	Brett Lonsdale	Read	 DAppTest3 Visitors
DAppTest3	Brett Lonsdale	Limited Access	 DAppTest3 Visitors
DAppTest3	Brett Lonsdale	Read	 DAppTest3 Visitors
DAppTest3	Brett Lonsdale	Limited Access	 DAppTest3 Visitors
DAppTest3	Brett Lonsdale	Edit	 DAppTest3 Members
DAppTest3	Brett Lonsdale	Limited Access	 DAppTest3 Members
DAppTest3	Brett Lonsdale	Limited Access	 Brett Lonsdale

[<< Discover Permissions Results](#)

[Other Reports >>](#)

Other Reports

The [DeliverPoint SharePoint Online Add-In for Office 365 Professional](#) offers additional reporting for discovering unique permissions and comparing permissions.

The [Unique Permissions Report](#) discovers SharePoint Online objects to which a user, Active Directory Group or SharePoint Group has been given explicit permissions. In other words, this report is run against a user account or group (Account Centric) to display locations that have had their permission inheritance removed in order for custom permissions to be applied.

The [Compare Permissions Report](#) allows the user to compare permissions between two or more sites.

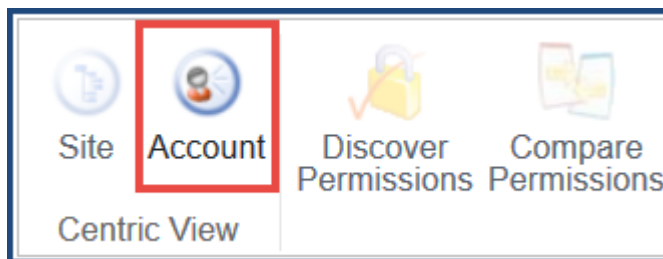
[<< Refining Discover Permissions Results](#)


[Unique Permissions Report \(Account Centric View\) >>](#)

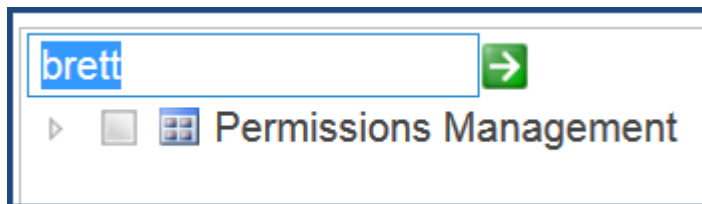
Unique Permissions Report (Account Centric View)

To use the **Unique Permissions** command, complete the following steps:

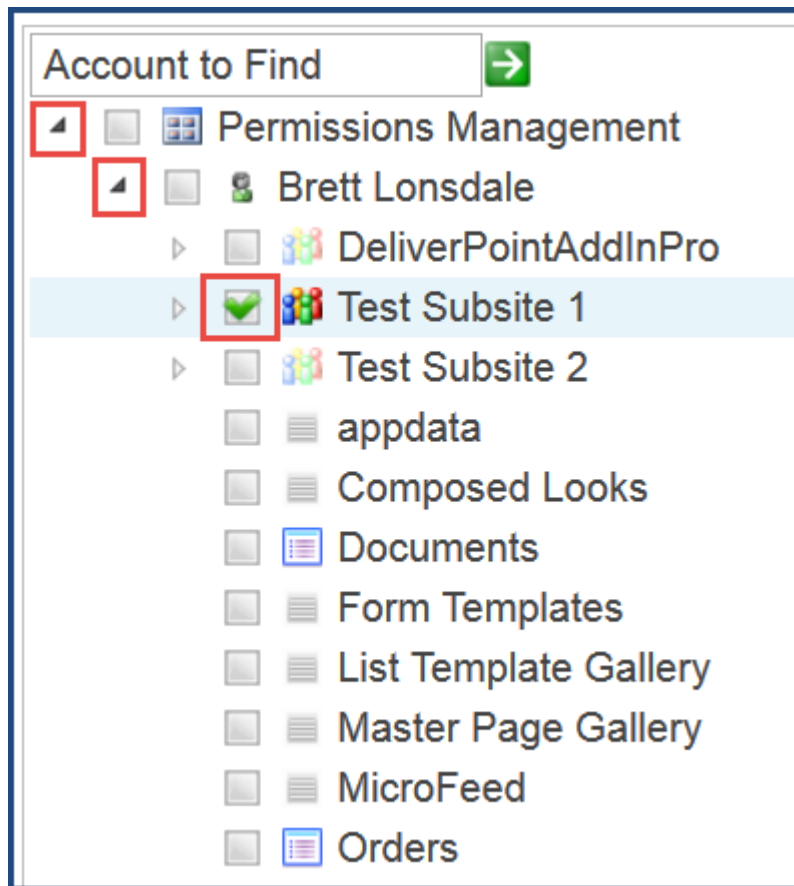
1. Navigate to the **DeliverPoint Add-In Main Page**.
2. Click **Account** under the **Centric View** section in the ribbon.



3. In the *Account to find* search box, type one or more characters of a username and then click the  white arrow with a green background icon.



4. In the tree view, expand **Permissions Management** and select the username to be included in the scope. Or, expand further below a username and select a SharePoint object, such as a Site Collection or List (as shown below).













5. On the **Reporting** section in the Ribbon, click **Unique Permissions**.




The *Discover Permissions with DeliverPoint Add-In Main Page* is displayed.

Account Memberships

Account	Member Account
 Brett Lonsdale	
 Migration tool	Brett Lonsdale
 Partners	Brett Lonsdale
 Pizza	Brett Lonsdale
 Sales Group	Brett Lonsdale
 Technical Support	Brett Lonsdale
 TestParentGroup	Brett Lonsdale
 Usergroup	Brett Lonsdale
 DPAppTest3 Members	Brett Lonsdale
 Test Subsite 1 Members	Brett Lonsdale

Unique Site Permissions

Account	Site	Permission
 Test Subsite 1 Members	Test Subsite 1	Edit

Unique List Permissions

Account	Parent Site	List	Permission
---------	-------------	------	------------

The report displays information in the following sections:

- **Account Membership.** The Account, Defining Site Collection and Member Account.
- **Unique Site Permissions.** The Account, Site, and Permission Level.
- **Unique List Permissions.** The Account, Site, List Name, and Permission Level.



The Site, List, and Permission Level are all hyperlinks, and when clicked open the respective page. For example, clicking on the Site hyperlink opens the root page of the site, and clicking on the Permission Level opens the Edit Permissions page.

You can save the report. In the results pane, on the **Reporting** section in the ribbon and click **Export to CSV**. The Microsoft® Excel spreadsheet file name is of the format, *ExportDiscoveredPermissions_yyyy-mm-ddXXX.csv*, where XXX is the timestamp unique for each file.

[<< Other Reports](#)

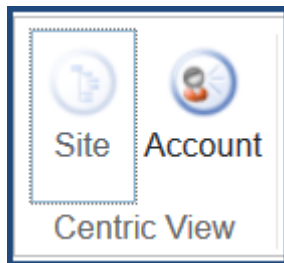
[Compare Permissions Report >>](#)

Compare Permissions Report

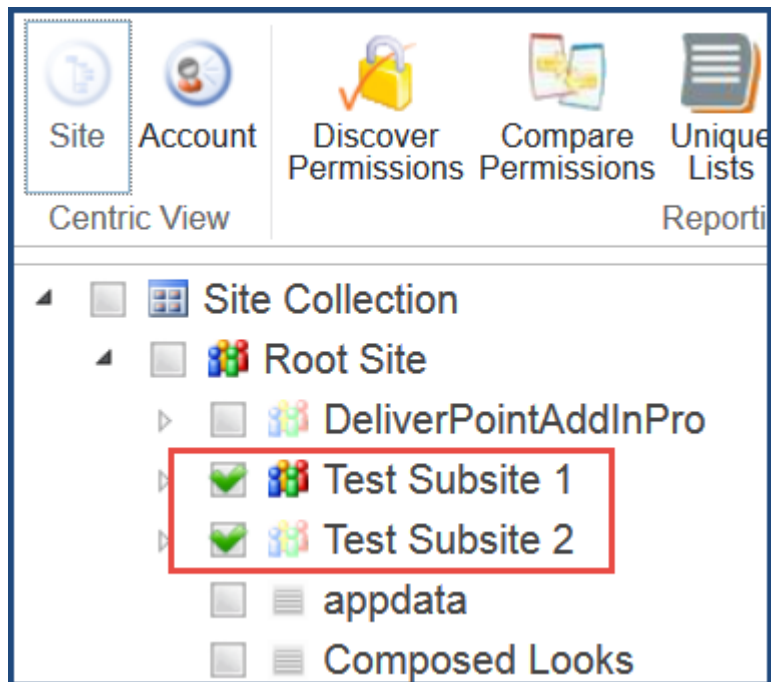
To use the **Compare Permissions** action, complete the following steps:

! This DeliverPoint action can only be used to compare Site permissions.

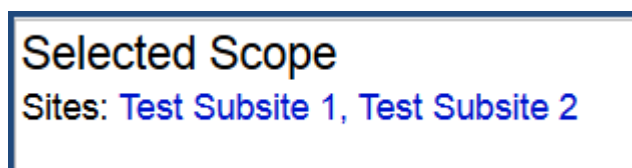
1. Navigate to the **DeliverPoint Add-In Main Page**.
2. In the ribbon, ensure that the **Site Centric View** is selected. (This should be the default view when first navigating to the Add-In Main Page. The Site icon in the ribbon will be deactivated.)



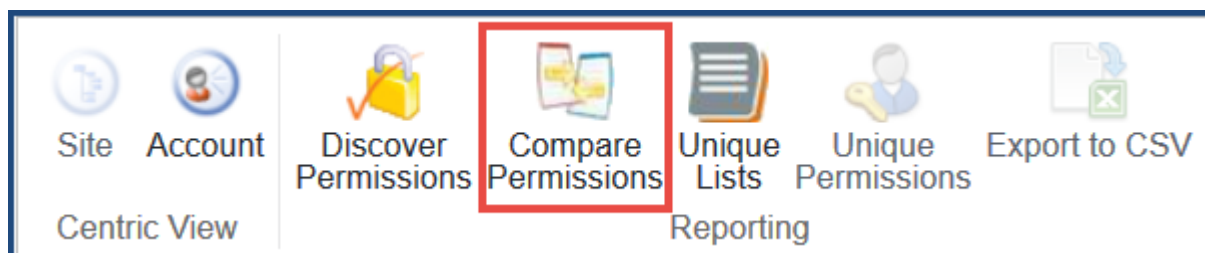
3. In the tree view, expand the top-level site collection and select one or more sites to be included in the scope. **Note:** *This action cannot be completed on accounts and child nodes are not automatically included.*




A summary of the selected objects are displayed in the *Selected Scope* pane below the tree view and results panes.



4. Under the **Reporting** section in the Ribbon, click **Compare Permissions**.



If you only select one site, then the *Compare Permissions* command is inactive, you must select at least 2 sites where you have the *Enumerate Permissions* rights before this command is available to you on the Ribbon. Sites have been designated with the  icon.

The results are displayed in the *DeliverPoint Add-In Main Page Results* pane. The nodes included in

the scope are displayed as column headings.

Username	Test Subsite 1	Test Subsite 2
Test Subsite 1 Owners	Full Control	.
Test Subsite 1 Members	Edit	.
Test Subsite 1 Visitors	Read	.
Excel Services Viewers	.	View Only
DPAppTest3 Owners	.	Full Control
DPAppTest3 Visitors	.	Read Limited Access
DPAppTest3 Members	.	Edit Limited Access
Karen Khumaryan	.	Limited Access

To export the report, on the Ribbon in the **Reporting** section, click **Export to CSV**. The Microsoft® Excel spreadsheet file name is of the format, *ExportComparedPermissions_yyyy-mm-ddXXX.csv*, where XXX is the unique timestamp for the file.

[<< Unique Permissions Report \(Account Centric View\)](#)
[Managing Permissions >>](#)

Managing Permissions

The DeliverPoint Add-In allows you to manage SharePoint permissions in a Microsoft® Office 365 SharePoint Online environment. From the tree view on the *DeliverPoint Add-In Main Page*, by clicking a SharePoint object, you can initiate DeliverPoint tasks which are displayed on the DeliverPoint Add-In Ribbon and divided into groups: **Centric View**, **Reporting**, **Management**, and **General**. The Management actions you can complete are listed below.

✿ Not all actions can be completed on all SharePoint objects.

- [Copy Permissions](#)
- [Grant Permissions](#)
- [Transfer Permissions](#)
- [Delete Permissions](#)
- [Inherit Permissions](#)
- [Break Permissions](#)

The Copy, Delete, and Transfer Permissions actions use Office 365 Active Directory user or group accounts, or SharePoint groups.

[<< Compare Permissions Report](#)

[Copy Permissions >>](#)

Copy Permissions

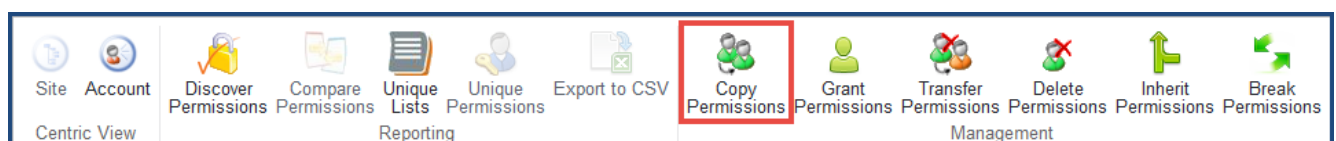
When you choose to use the **Copy Permissions** command, changes will be applied to all sites, lists, folders, and list items in the selected scope(s), where you are able to manage SharePoint permissions. If you are not able to manage permissions for a specific site, folder, list or list item, changes will not be applied to that object.

✿ The DeliverPoint Add-In will not at any time enumerate membership of an Active Directory group during the **Copy Permissions** operation.

The source permission rights are appended to the existing permissions for the target account(s). The effect of appending permission rights is that none of the existing permissions for the target account(s) are replaced or deleted. Instead, the permissions are given to the target account in addition to existing permissions. For example, if the target account has **Read** permissions on *Site A* and the source account has **Contribute** permissions on *Site A*, then the target account's permissions in *Site A* will now include **Contribute**. However, if in *Site B* the target account's permissions are **Design** and the source account's permissions are **Read**, then the target account's permission will retain the higher permission level of **Design** while still receiving the new **Read** permission level. In other words, permissions are appended and not replaced in the copy operation.

To use the **Copy Permissions** command:

1. Navigate to the [DeliverPoint Add-In Main Page](#).
2. On the Ribbon in the **Centric View** section, click either the **Site** or **Account**.
3. In the tree view, select those nodes, also known as SharePoint objects, to be included in the scope. For example, select one or more sites or an account. The summary of the nodes selected are displayed in the *Selected Scope* pane below the *Tree View* and *Results* panes. **Note:** *Child nodes are not automatically included*.
4. On the Ribbon, click **Copy Permissions** in the **Management** group.



The *Results* pane on the *DeliverPoint Add-In Main Page* displays further configuration options required for copying permissions. The selected scope will be displayed at the top of the *Results* pane.

5. Complete information in the following sections:

- **From Account.** Use this section to identify the source usernames, domain group names or email address of the account (source) you wish to use as a basis for the copy operation.

From account You can enter a username, domain group name, e-mail address or SharePoint group name.	<input type="text" value="brett"/> Brett Lonsdale Showing 1 result
--	--

- **To Account.** Use this section to identify the target usernames, domain group names, or email address.

To account You can enter usernames, domain group names or e-mail addresses. Separate them with semicolons.	<input type="text" value="sandy"/> Sandy Ussia Showing 1 result
---	---

- **To SharePoint group.** Use this section to enter SharePoint groups as the targets.
- **Process.** Select or deselect the following options:
 - Include sub site(s)
 - Include list(s)
 - Include list item(s)
 - Break permissions inheritance if required
 - Detailed log (*Selected by default*)

Once the above information is completed, click the **Copy** button.

Copy Permissions

Use this page to copy permissions from users or groups to another set of users or groups. Changes will be applied to all sites, lists and list items within the selected scope.

Scope
Actions will be applied to the specified scope.

From account
You can enter a username, domain group name, e-mail address or SharePoint group name.

To account
You can enter usernames, domain group names or e-mail addresses. Separate them with semicolons.

To SharePoint group
You can enter SharePoint group names. Separate them with semicolons.

Process
Specify settings to control the process.

List: **Old Documents**

☐ Include sub site(s)
☐ Include list(s)
☐ Include list item(s)
☐ Break permissions inheritance if required
☒ Detailed Log

The *Results* pane then displays a message that the jobs have completed successfully.

Process completed successfully.

If you wish to see more details of the operation, click **Show Details**. This will display information such as To and From Accounts or Groups, process options that were selected, processing sites/lists, and permission changes made.

Manage permissions process log

Selected manage action: **Copy Permissions**

Process settings

From user: **i:0#.f|membership|brett@lightningtools365.onmicrosoft.com**

To users: **i:0#.f|membership|sandy@lightningtools365.onmicrosoft.com**

To groups:

Include children sites: **false**

Include children lists: **false**

Include list items: **false**

Break inheritance if needed: **false**

Scope: selected sites and lists

Processing sites**Processing lists**

Processing list: **Old Documents** of site: **DPAppTest3**

Adding **Edit** to user **Sandy Ussia**

Process completed successfully

[<< Managing Permissions](#)

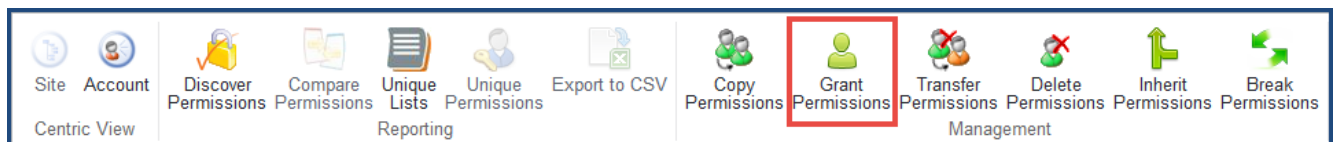
[Grant Permissions >>](#)

Grant Permissions

Using this DeliverPoint permission command, you can grant permissions at a SharePoint object level, such as a site, list, library, list item, or file, as well as to one or more usernames, email addresses, Active Directory groups or SharePoint groups, or a combination, which you then map to a permission level or SharePoint Group.

To use the **Grant Permissions** command, complete one of the three following methods:

1. Navigate to the [DeliverPoint Add-In Main Page](#) and select either **Site** or **Account** from the Centric View section in the Ribbon.
2. In the tree view, select those nodes, also known as SharePoint objects, to be included in the scope. For example, select one or more sites or an accounts. A summary of the node[s] selected are displayed in the *Selected Scope* pane below the *Tree View* pane. **Note:** *Child nodes are not automatically included.*
3. On the Ribbon, click **Grant Permissions** in the **Management** group.



The *Grant Permissions* page is displayed to the right of the *Tree View*. The nodes included in the scope are displayed at the top of the page.

4. Complete information in the following sections:
 - **To Account.** Use this section to identify the target usernames, Active Directory groups, SharePoint Groups or email address of the account (source) you wish to use as a basis for the grant operation. Once you start typing in the box, you should receive suggestions

To account You can enter usernames, domain group names or e-mail addresses. Separate them with semicolons.	<input type="text" value="sandy"/> <div>Sandy Ussia</div> <div>Showing 1 result</div>
---	--

- **To SharePoint Group.** Use this section to identify a SharePoint group as the target.
- **Permissions.** Use this section to select the permission level(s). The permission levels that are displayed in this section are dependent on the permission levels defined for your scope.

Permissions Select permissions to be granted.	<input type="checkbox"/> Full Control <input type="checkbox"/> Design <input type="checkbox"/> Edit <input type="checkbox"/> Contribute <input type="checkbox"/> Read <input type="checkbox"/> View Only
---	---

- **Groups.** Use this section to add SharePoint Groups that the accounts must be added to in order to grant permissions. Once typing begins in the box, you will be offered suggestions.

Groups Select groups to which the accounts must be added in order to grant permissions.	DPAp
Process Specify settings to control the process.	DPApTest3 Members DPApTest3 Owners DPApTest3 Visitors Showing 3 results

- **Process.** Select or deselect the following options.
 - Include sub site(s)
 - Include list(s)
 - Include list item(s)
 - Break permissions inheritance if required
 - Detailed log (*Selected by default*)

Process Specify settings to control the process.	<input type="checkbox"/> Include sub site(s) <input type="checkbox"/> Include list(s) <input type="checkbox"/> Include list item(s) <input type="checkbox"/> Break permissions inheritance if required <input checked="" type="checkbox"/> Detailed Log
--	---

Review and then click **Grant**.

The *Results* pane then displays a message that the process completed successfully.

Process completed successfully.

Show details

If you wish to see more details of the operation, click **Show Details**. This will display information such as To and From Accounts or Groups, process options that were selected, processing sites/lists, and permission changes made.

Manage permissions process log

Selected manage action: **Grant Permissions**

Process settings

To users: **i:0#.f|membership|brett@lightningtools365.onmicrosoft.com**

To groups:

Add to groups: **DPAppTest3 Visitors**

Include children sites: **false**

Include children lists: **false**

Include list items: **false**

Break inheritance if needed: **false**

Scope: selected sites and lists

Looking for subsites and lists in site: **DPAppTest3**

Processing sites

Processing site: **DPAppTest3**

Adding **Brett Lonsdale** user to group **DPAppTest3 Visitors**

Processing lists

Process completed successfully

[<< Copy Permissions](#)

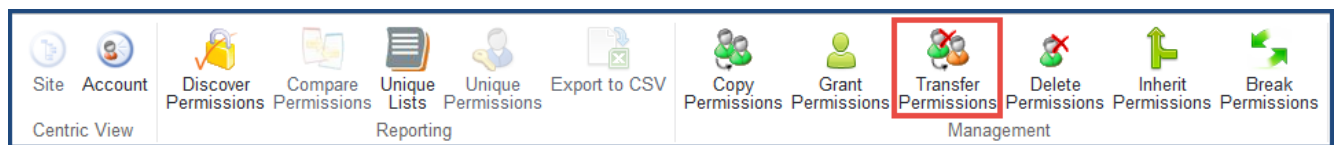
[Transfer Permissions >>](#)

Transfer Permissions

DeliverPoint allows you to select a scope, copy the permission set of an account (source) within that scope to other account(s) (target), and then the source account is deleted within the selected scope. This operation is a combination of the [Copy Permissions](#) and [Delete Permissions](#) commands.

To use the **Transfer Permissions** command:

1. Navigate to the [DeliverPoint Add-In Main Page](#) and select either **Site** or **Account** from the Centric View section in the ribbon.
2. In the tree view, select those nodes, also known as SharePoint objects, to be included in the scope. For example, select one or more sites, lists, or an account. A summary of the node[s] selected are displayed in the *Selected Scope* pane below the Tree View. **Note:** *Child nodes are not automatically included.*
3. On the Ribbon, click **Transfer Permissions** in the **Management** group.



The *Transfer Permissions* page is displayed. The nodes included in the scope are displayed below the page title.

4. Complete information in the following sections. You may need to scroll down to see all the sections:
 - **From Account.** Use this section to identify the source usernames, groups or email address of the account (source) you wish to use as a basis for the transfer operation. The source account is the account from which the permissions are to be copied from, and the account to be subsequently deleted.

Once you begin typing in the box, you will be offered suggestions. **Note:** *Only one username, Active Directory group or SharePoint Group can be specified.*

From account You can enter a username, domain group name, e-mail address or SharePoint group name.	br	
	Brett Lonsdale	
	Showing 1 result	

- **To Account.** Use this section to identify one or more target usernames, Active Directory groups, SharePoint Groups, email address, or a combination. The target is the account[s] to whom the permissions will be copied to. The DeliverPoint Add-In allows multiple target accounts to be added in one job.

To account You can enter usernames, domain group names or e-mail addresses. Separate them with semicolons.	Sandy Ussia x Sara Lonsdale x	

- **To SharePoint Group.** Use this section to specify one or more SharePoint groups as the target.

To SharePoint group You can enter SharePoint group names. Separate them with semicolons.	dpapp	
	DPAppTest3 Members	
	DPAppTest3 Owners	
Process Specify settings to control the process.	DPAppTest3 Visitors	
	Showing 3 results	

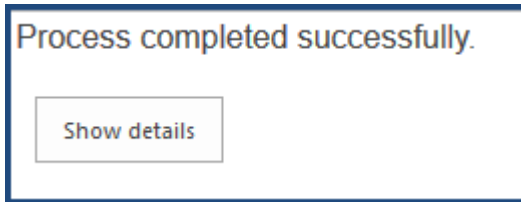
- **Process.** Select or deselect the following options:

- Include Subsite[s]
- Include List[s]
- Include List item[s]
- Break permission inheritance if required
- Detailed log (*Selected by default*)

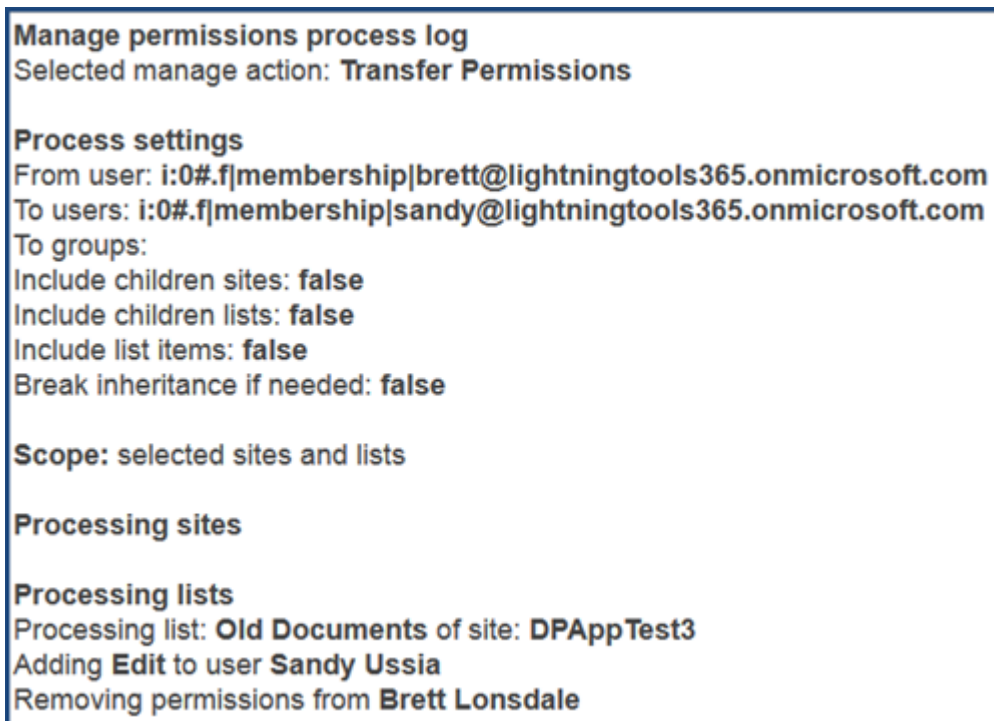
Process Specify settings to control the process.	<input type="checkbox"/> Include sub site(s)
	<input type="checkbox"/> Include list(s)
	<input type="checkbox"/> Include list item(s)
	<input type="checkbox"/> Break permissions inheritance if required
	<input checked="" type="checkbox"/> Detailed Log

Review the page and then click **Transfer**.

The *Results* pane then displays a message that the process completed successfully.



If you wish to see more details of the operation, click Show Details. This will display information such as To and From Accounts or Groups, process options that were selected, processing sites/lists, and permission changes made.



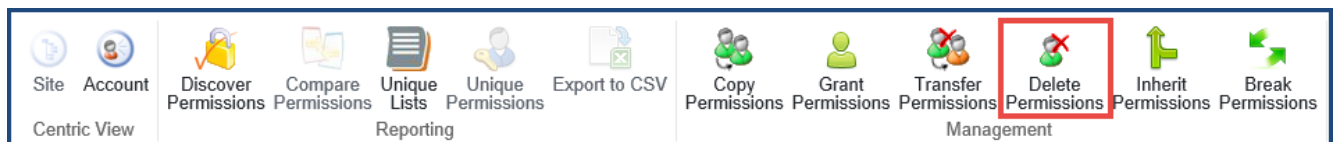
[<< Grant Permissions](#)

[Delete Permissions >>](#)

Delete Permissions

To use the **Delete Permissions** command, complete the following steps:

1. Navigate to the [DeliverPoint Add-In Main Page](#) and select either the **Site** or **Account** from the Centric View section in the ribbon.
2. In the tree view, select those nodes, also known as SharePoint objects, to be included in the scope. For example, select one or more sites, lists, or an account. The summary of the nodes selected are displayed in the *Selected Scope* pane below the Tree View. **Note:** *Child nodes are not automatically included.*
3. On the Ribbon, click **Delete Permissions** in the **Management** group.



The *Delete Permissions* page is displayed in the results pane. The nodes included in the scope are display below the page title.

4. Complete information in the following sections:
 - **From Account.** Use this section to identify the target usernames, Active Directory groups, SharePoint Groups, or email address of the account (source) you wish to delete permissions. Once you begin typing in the box, you should receive suggestions.

From account You can enter a username, domain group name, e-mail address or SharePoint group name.	<input type="text" value="brett"/> <div> Brett Lonsdale Showing 1 result </div>
--	---

- **Process.** Select or deselect the following options:
 - Include Subsite[s]
 - Include List[s]
 - Include List item[s]

- Break permission inheritance if required
- Detailed log (*Selected by default*)

Process Specify settings to control the process.	<input type="checkbox"/> Include sub site(s) <input type="checkbox"/> Include list(s) <input type="checkbox"/> Include list item(s) <input type="checkbox"/> Break permissions inheritance if required <input checked="" type="checkbox"/> Detailed Log
--	---

Review and click **Delete**.

The *Results* pane then displays a message that the process completed successfully.

Process completed successfully.

Show details

If you wish to see more details of the operation, click **Show Details**. This will display information such as To and From Accounts or Groups, process options that were selected, processing sites/lists, and permission changes made.

Manage permissions process log
Selected manage action: **Delete Permissions**

Process settings
From user: i:0#.f|membership|brett@lightningtools365.onmicrosoft.com
Include children sites: **false**
Include children lists: **false**
Include list items: **false**
Break inheritance if needed: **false**

Scope: selected sites and lists

Processing sites

Processing lists
Processing list: **Old Documents** of site: **DPAppTest3**

Process completed successfully

[<< Transfer Permissions](#)
[Permissions Inheritance >>](#)

Permissions Inheritance

For easier administration, it is recommend that you avoid breaking inheritance too frequently. That is, you should keep the permissions inheritance intact for all sites, lists, libraries, and items. To avoid breaking inheritance at the list, library, list item, or file level, you should organize sites so that you can assign permissions to the site that contains the protected content. For example, you might create a sub site for documents that contain sensitive data, or a sub site that contains lists with restricted access. In this way, you can manage permissions for all content in a site with one action, instead of tracking many individual documents or list items. (See the white paper, [Best practices for using fine-grained permissions](#).)

If you believe permission inheritance has been broken at the list, library, list item or file levels, then you can use the [Unique Permissions](#) DeliverPoint Add-In commands to find where permission inheritance was stopped and different permissions assigned.



A site collection is a security boundary, that is, the top-level site of the site collection, and it does not inherit its permission settings from any other site. The site collection administrator configures the initial permissions settings for a site collection, which are then inherited by the content in the site collection (sites, lists, libraries, list items and files). *The DeliverPoint Add-In can only manage permissions within the scope of a single Office 365 SharePoint Online Site Collection.*

You can use the DeliverPoint Add-In to manage site, list, folder, or item-level permission inheritance. You can use the Permission Inheritance DeliverPoint Add-In commands, [Inherit Permissions](#) and [Break Permissions](#), from the [DeliverPoint Add-In Main Page](#).

[<< Delete Permissions](#)

[Inherit or Break Permissions >>](#)

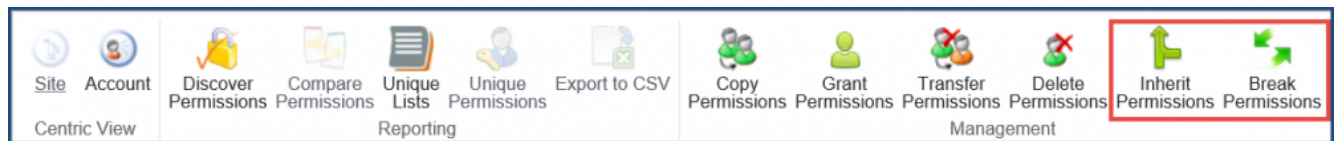
Inherit or Break Permissions

To modify [Permission Inheritance](#) from the [DeliverPoint Add-In Main Page](#), complete the following steps:

1. Navigate to the [DeliverPoint Add-In Main Page](#) and click either the **Site** or **Account** in the Centric View section of the ribbon.
2. In the Tree View, select those sites to be included in the scope. If lists and libraries are displayed in the Tree View, you can also select a list or library. **Note:** *The Inherit Permissions and Break Permissions commands cannot be used on accounts.*

The summary of the node(s) selected are displayed in the *Selected Scope* pane below the Tree View.

3. On the Ribbon, click either **Inherit Permissions** or **Break Permissions** from the **Management** group. **Note:** *When you select Inherit Permissions, you will lose any unique permission settings that you have configured on that object (site, list/library, item/file).*



The *Break Permissions* or *Inherit Permissions* page is displayed in the results pane. The scope of the operation is displayed below the title.

Inherit Permissions

Use this command to selected content inherit their permissions from parent. Changes will be applied to all sites and lists within the selected scope.

All descendant objects of sites on which this method is run will also start inherit from their parent site, not just the immediate children.

Sub sites with unique permissions will be ignored during the process.

Scope

Actions will be applied to the specified scope.

List: **Old Documents**

Process

Specify settings to control the process.

☐ Include sub site(s)

☒ Detailed Log

Inherit

Cancel

4. Optionally select or deselect **Process** options to include subsites and/or lists, or to include a detailed log. **Note:** *Detailed log is selected by default.*
5. Click **Break** or **Inherit**.

The *Results* pane then displays a message that the process completed successfully.

Process completed successfully.

Show details

If you wish to see more details of the operation, click **Show Details**. This will display information such as scope, process options that were selected, processing sites/lists, and permission changes made.

Manage permissions process log

Selected manage action: **Inherit Permissions**

Process settings

Include children sites: **false**

Scope: selected sites and lists

Processing sites**Processing lists**

Processing list: **Old Documents** of site: **DPAppTest3**

Enabling permissions inheritance of SOP: list: **Old Documents**

Process completed successfully

[<< Permissions Inheritance](#)

[Return to Managing Permissions](#)