|  |
| --- |
|  |
| SharePoint Permission Manager 2015™ |
| User Manual |
|  |
|  |
| **6/20/2016** |

|  |
| --- |
|  |

This document will provide users with instructions on how to use QIPoint’s SharePoint Permission Manager™ tool.

Table of Contents

[Introduction 4](#_Toc454223033)

[Installation & Minimum Requirements 5](#_Toc454223034)

[IMPORTANT: This program does not need to be installed on a SharePoint Server. 5](#_Toc454223035)

[Minimum Hardware Recommendations 5](#_Toc454223036)

[Supported SharePoint Versions 5](#_Toc454223037)

[.NET Framework Required 5](#_Toc454223038)

[Local Machine & Windows System Permissions Required 7](#_Toc454223039)

[Anti-Virus, Offline Sync Folders (i.e. Google Drive, OneDrive, Drop Box, etc) and Performance 7](#_Toc454223040)

[SharePoint User Permissions Required 8](#_Toc454223041)

[Full Permissions Reporting 8](#_Toc454223042)

[Limited Permissions Reporting: 8](#_Toc454223043)

[Office 365 Accounts 8](#_Toc454223044)

[Reports Overview 10](#_Toc454223045)

[Overview - Types of Permissions Reports 10](#_Toc454223046)

[1. All Site, List & Item Level Permissions 10](#_Toc454223047)

[2. Check User Permissions 10](#_Toc454223048)

[3. Orphaned User Accounts 11](#_Toc454223049)

[How to Create a Permissions Report 11](#_Toc454223050)

[Summary 11](#_Toc454223051)

[Create the Report 11](#_Toc454223052)

[Scan Options 13](#_Toc454223053)

[*Job Name* 13](#_Toc454223054)

[*Site URL* *to Scan* 13](#_Toc454223055)

[*Credentials* 13](#_Toc454223056)

[*Use Proxy Server* 13](#_Toc454223057)

[*Report Options* 13](#_Toc454223058)

[Email and Export 14](#_Toc454223059)

[Report: Check User Permissions 15](#_Toc454223060)

[Summary 15](#_Toc454223061)

[Checking a User’s Permissions 15](#_Toc454223062)

[Email and Export 16](#_Toc454223063)

[Report: Orphaned User Accounts 17](#_Toc454223064)

[Summary 17](#_Toc454223065)

[Checking for Orphaned Users 17](#_Toc454223066)

[Report: Email and Export Options 19](#_Toc454223067)

[*Email* 19](#_Toc454223068)

[Export 19](#_Toc454223069)

[Opening the Report 20](#_Toc454223070)

[Editing Permissions 20](#_Toc454223071)

[How to schedule removal of User Accounts (from Site/List or Item Level) 21](#_Toc454223072)

[Scheduling Scan Jobs (Enterprise version only) 24](#_Toc454223073)

[Schedule a Job 24](#_Toc454223074)

[Viewing & Managing Scheduled Jobs 25](#_Toc454223075)

[Licensing 26](#_Toc454223076)

[Components 26](#_Toc454223077)

[Changing the license type of a component 26](#_Toc454223078)

[Obtaining a License 26](#_Toc454223079)

[Transferring a License 26](#_Toc454223080)

[Customizing Permission Reports 27](#_Toc454223081)

[Site Permissions Report 27](#_Toc454223082)

[List Permissions Report 27](#_Toc454223083)

[Summary 27](#_Toc454223084)

[Sample Reports 27](#_Toc454223085)

[Grid View Report 28](#_Toc454223086)

[Customizing the Report 28](#_Toc454223087)

[Filtering 28](#_Toc454223088)

[Advanced Filtering 28](#_Toc454223089)

[Searching within the Report 29](#_Toc454223090)

[Filtering Queries 29](#_Toc454223091)

[Grouping 31](#_Toc454223092)

[Editing User / Group Permissions 32](#_Toc454223093)

[Manually Updating User / Group Permissions 32](#_Toc454223094)

[Automatically Updating User / Group Permissions 32](#_Toc454223095)

[Permission Templates – “Save Job” 35](#_Toc454223096)

[Report Archive 38](#_Toc454223097)

[Technical Support 39](#_Toc454223098)

[Version Comparison 39](#_Toc454223099)

# Introduction

This utility is a part of the SharePoint Essentials Toolkit TM Suite. This utility is used to manage and help report on SharePoint permissions.

Specifications

# Installation & Minimum Requirements

Please see the “SharePoint Essentials Toolkit – User Guide” for installation instructions.

## IMPORTANT: This program does not need to be installed on a SharePoint Server.

## Minimum Hardware Recommendations

**Processor:** Minimum Dual-Core, 3GHz. Recommended Quad-Core 3GHz or higher  
We recommend Quad-Core 3GHz processor or higher when scheduling more than 20 Jobs at one time.

**RAM:** Minimum 4GB. Recommended 8GB or higher  
We recommend at least 4GB of available RAM for sites less than 200GB and less than 10K items to scan, 6GB RAM free for sites with 200GB to 500GB or with 10-100K items to scan, 8+GB available RAM for sites with 500GB+ or with 100K items or more to scan. NOTE: You can reduce the RAM required by breaking down URL scan jobs into separate smaller jobs, such as create a single job per List/Library to run at different time intervals (rather than all Lists/Libraries at once in a single job which would require more memory/RAM utilization).

**Hard Disk:** 200MB Available Hard Disk Space (for the application files, logs, temp files and reports).   
Temp files are automatically cleared as needed. This is in addition to the disk space required by the SharePoint Essentials Toolkit.

## Supported SharePoint Versions

Microsoft SharePoint Office 365  
Microsoft SharePoint Server 2016  
Microsoft SharePoint Foundation 2013   
Microsoft SharePoint Server 2013  
Microsoft SharePoint Foundation 2010  
Microsoft SharePoint Server 2010

## .NET Framework Required

.NET Framework 4.5 or higher is required. If it is not found on the client machine, the user will be prompted to automatically download and install the prerequisite.



## Local Machine & Windows System Permissions Required

Please see the SharePoint Essentials Toolkit User Manual.

## Anti-Virus, Offline Sync Folders (i.e. Google Drive, OneDrive, Drop Box, etc) and Performance

Please see the SharePoint Essentials Toolkit User Manual.

# SharePoint User Permissions Required

Users require specific SharePoint permissions to be able to use the tool, see below for the specific permission levels required:

## Full Permissions Reporting

Providing the permission levels below will allow a user to report on all permissions. This provides the full features of the tool. The user must be either:

* A member of “Site Collection Administrators” group
* Or have Full Control at Web Application level user policy

## Limited Permissions Reporting:

Providing the permission levels below will allow a user to report on permissions that are ‘Directly Given’ only. They will not be able to enumerate users within groups. The “Show Nested Permissions” will be the only option that will not work and therefore users within SharePoint and AD Groups will not be visible in reports. If you need to report on nested permissions, grant permissions above (Site Collection Administrator) to the account running the tool.

**View Items -** View items in lists and documents in document libraries.

**Open Items -** View the source of documents with server-side file handlers.

**View Versions -** View past versions of a list item or document.

**View Application Pages -** View forms, views, and application pages. Enumerate lists.

**View Web Analytics Data -** View reports on Web site usage.

**Browse Directories** - Enumerate files and folders in a Web site using SharePoint Designer and Web DAV interfaces.

**View Pages -** View pages in a Web site.

**Enumerate Permissions -** Enumerate permissions on the Web site, list, folder, document, or list item.

**Browse User Information -** View information about users of the Web site.

**Use Remote Interfaces -** Use SOAP, Web DAV, the Client Object Model or SharePoint Designer interfaces to access the Web site.

**Open -** Allows users to open a Web site, list, or folder in order to access items inside that container.

## Office 365 Accounts

* When scanning Office 365 SharePoint sites, an Organizational account must be used, such as [user@mycompany.com](mailto:user@mycompany.com) or [user@mycompany.onmicrosoft.com](mailto:user@mycompany.onmicrosoft.com). Microsoft accounts (Windows Live IDs) such as [user@live.com](mailto:user@live.com) or [user@hotmail.com](mailto:user@hotmail.com), are not currently supported for authentication.

# Reports Overview

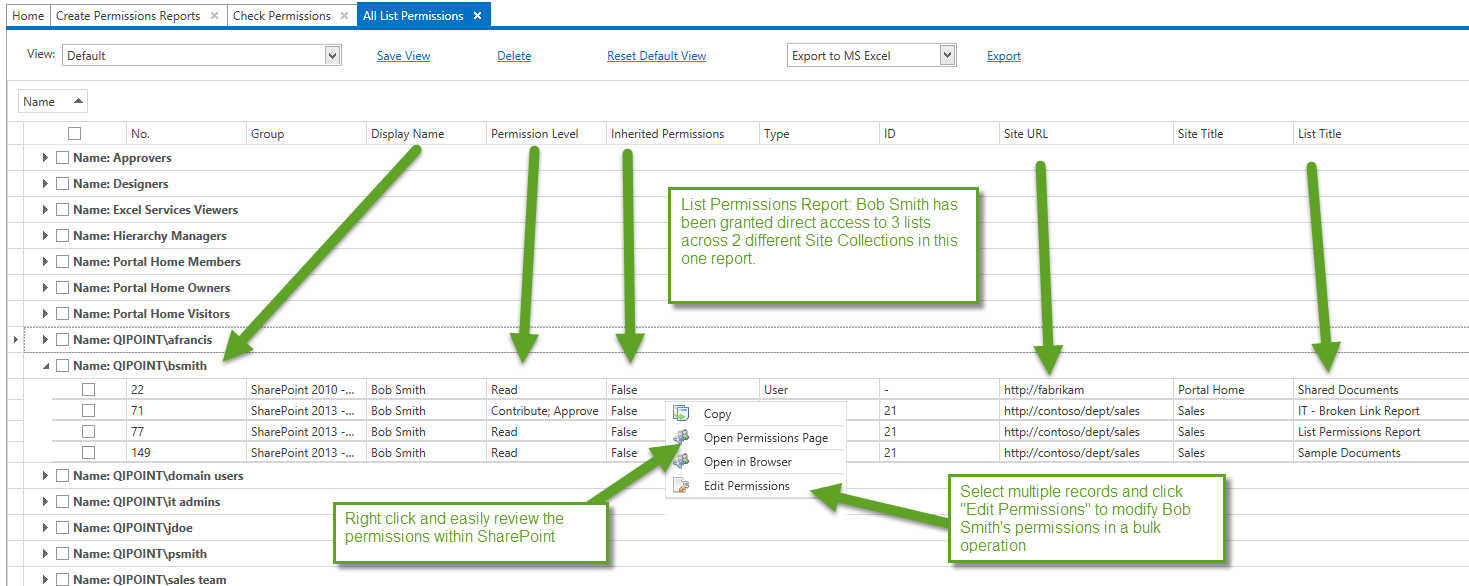
## Overview - Types of Permissions Reports

### All Site, List & Item Level Permissions

Performs a report on all site, list and unique item & folder level permission objects. This report will be blank if no previous site reports have been run.

This report is useful in gathering all permission settings across multiple sites, lists and items to analyze, compare and update as needed. This report can also aid in identifying unique permissions granted directly to user’s.

For example: You can build a report against multiple Site Collections, then group by a User Object such as QIPOINT\Sales Team or QIPOINT\bsmith and view all sites, list and items where this AD group or AD User has been assigned and change or remove as needed.

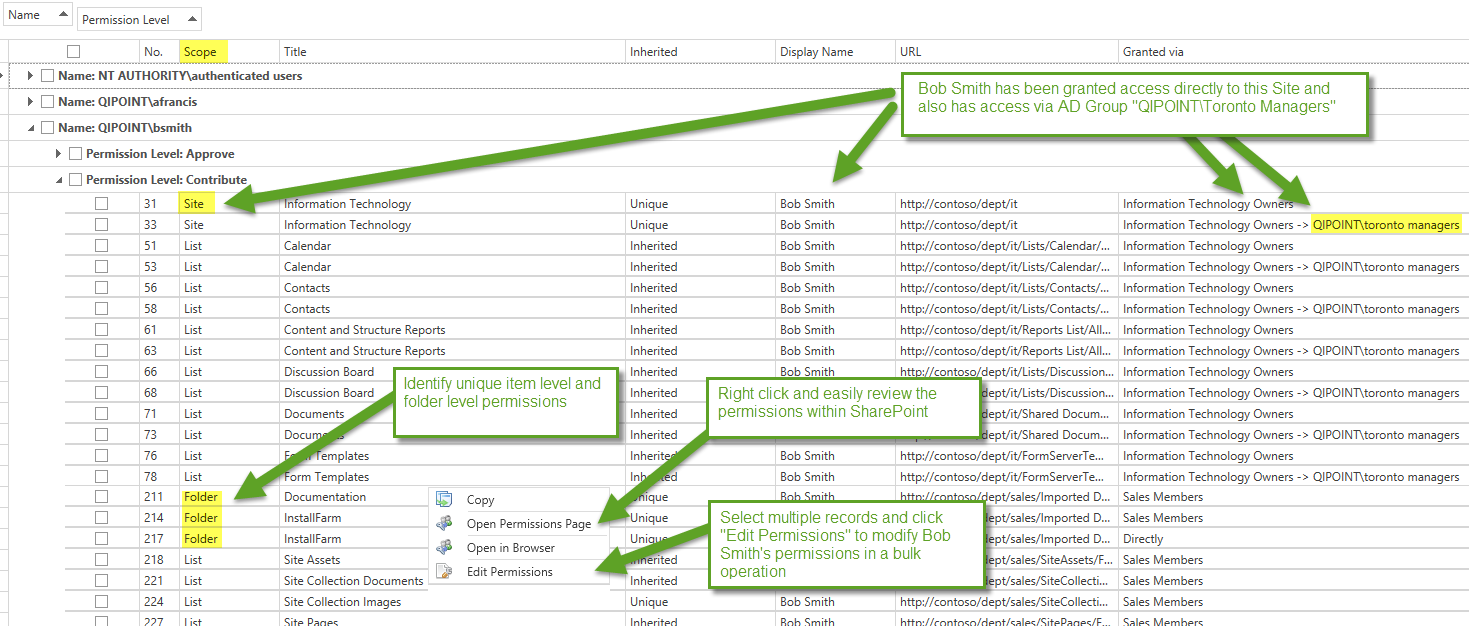


To create this type of report, click “Scan Site” from the Permissions tab.

### Check User Permissions

This report is used to identify all content that a user, AD group, or SharePoint Group has access to. If you are checking a user’s access, this will show access granted via SharePoint Group, AD Group membership or direct access (where the user was added directly to the site/list/item).

This type of report is different than the “Site, List & Item Permissions Audit” report (above) as it will only check permissions of the user/group entered. All SharePoint objects (sites, lists, items, folders) that the user has access to, will be displayed in one report.



To create this type of report, click “Check User Permissions” from the Permissions tab.

### Orphaned User Accounts

This creates a report that shows all orphaned users. An “Orphaned User” is a user object in SharePoint that does not have a corresponding AD Account. This could be a disabled or deleted AD user or group account.

To create this type of report, click “Check Orphaned Users” from the Permissions tab.

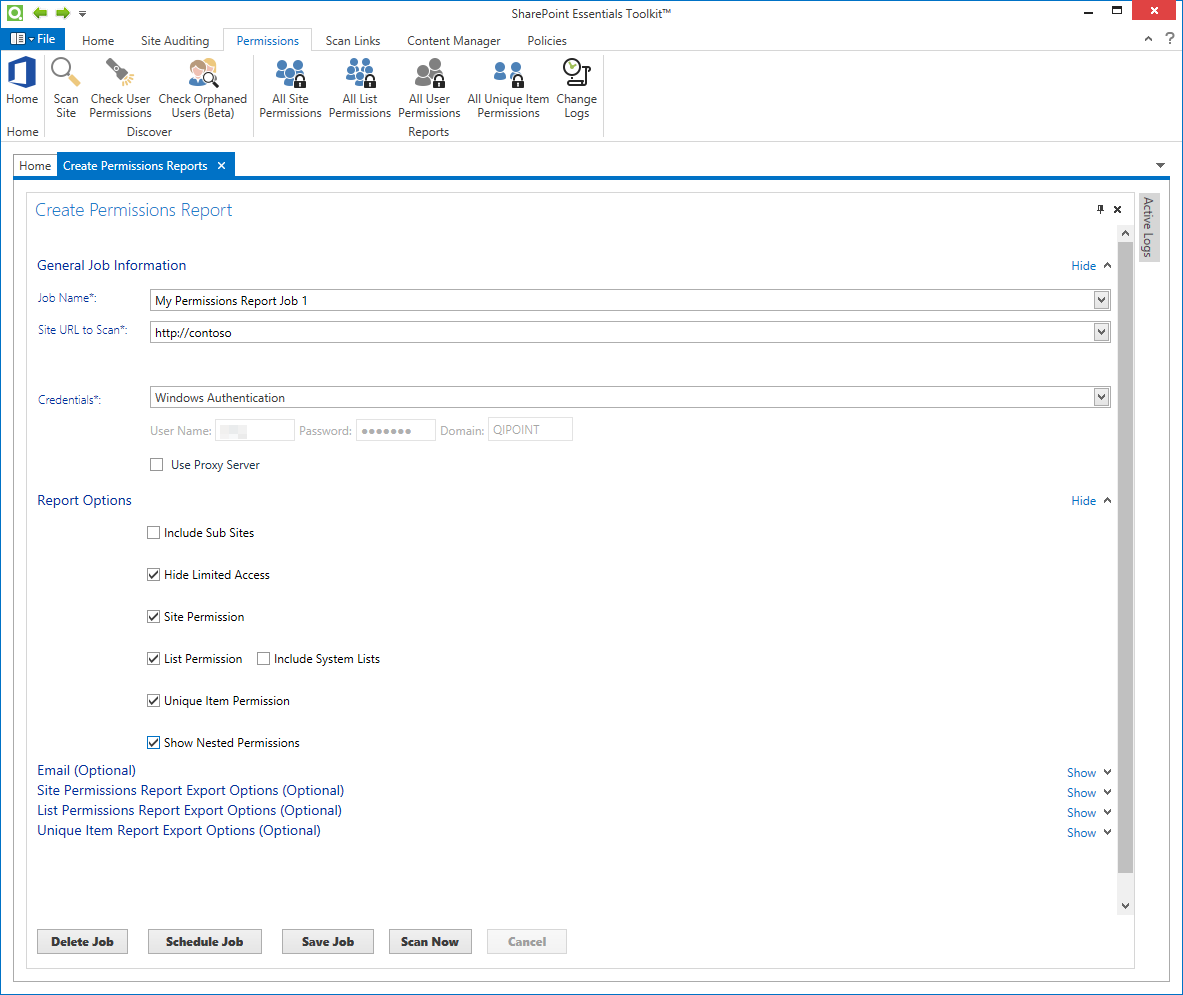
# How to Create a Permissions Report

## Summary

A permissions audit will scan a site and capture all permission objects contained within it. This includes all site level permissions, list permissions, and unique folder and item/file level permissions. This is useful in gathering all permission settings for the sites, lists and items within them to analyze, compare and update as needed.

## Create the Report

1. Open “SharePoint Essentials ToolkitTM”
2. Click on the “Permissions” tab at the top
3. Click on the “Scan Site” button
4. A new tab will appear called “Create Permissions Reports”



1. Complete the form. Fields with an asterisk \* indicate required fields

See “Report Options” (next section) for a description of each field.

1. Click “Scan Now” button to start the audit.

## Scan Options

### Job Name

This is the Name of the job. A folder will be created in the report directory for every job. You can use the same Job Name to group reports.

### Site URL to Scan

This is the absolute URL of the site you want to audit. This can be the path to a Site Collection or a sub site.  
  
**Example:** <https://companyportal/sites/hr>

### Credentials

Select the authentication type and enter the credentials used to access this site.

### Use Proxy Server

Select this option if you use a Proxy Server to access the SharePoint site you are scanning.

### Report Options

**Include Sub Sites** – The report will include all sub sites (under the site specified in ‘Site URL to Scan’).

**Hide Limited Access** – This will exclude limited access permission levels from appearing in the report. To read more about Limited Access see this article: <https://technet.microsoft.com/en-us/library/cc721640.aspx>

**Site Permission** – Select this option to build a report on Site permissions including users, groups and their respective permission levels.

**List Permission** – Select this option to build a report on List permissions including users, groups and their respective permission levels.

**Include System Lists** – Select this option to include hidden system lists in the List Permissions report.

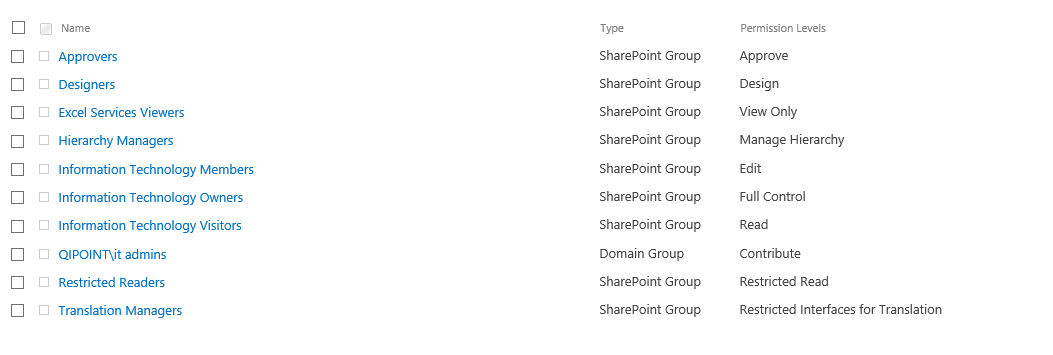
**Unique Item Permission** – Select this option to build a report on all items and folders that have unique permissions. The report identifies who has access to the items/folders and respective permission levels.

**Show Nested Permissions** – Select this option to display user and group (SharePoint and Active Directory Group) permissions nested within permission objects. For example: If this option is unchecked, only SharePoint Groups, AD Groups and Users will be displayed in the report that have been given access DIRECTLY in SharePoint, it will not display users or groups nested within the permission objects. If this option is turned on (checked), the tool will display all permission objects nested within any SharePoint Group or AD Group.

The column “Granted Through” will display if the user permissions was granted through one of these “Nested Permissions”

*Example:*

Below are permission objects for a site, if ‘Show Nested Permissions’ is disabled, only these objects will show in the report. If ‘Show Nested Permissions’ is enabled, these objects and all users and AD Groups within them will also appear in the reports.



### Email and Export

See “**Report: Email and Export Options**” section

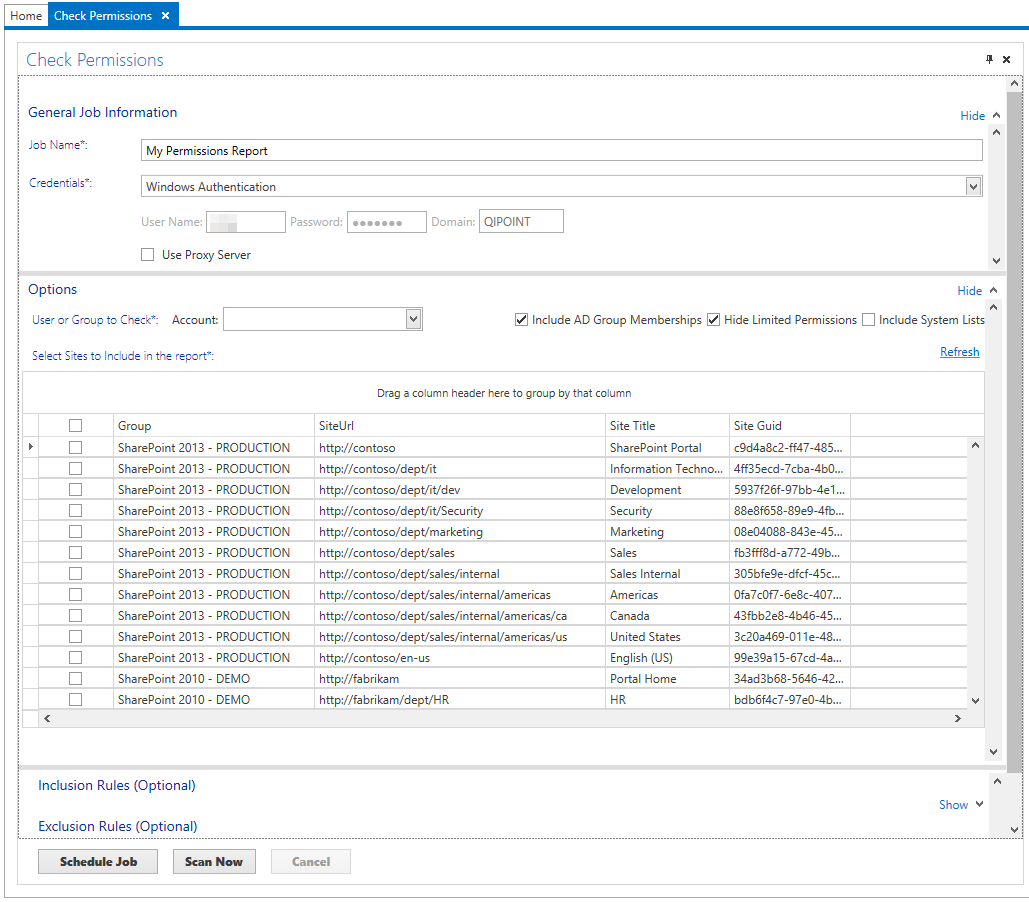
# Report: Check User Permissions

## Summary

This report will allow you to check a user’s permissions across multiple farms and sites collections. It will build an in –depth scan of the user’s access to anything within the specified site(s), including site, list and item level permissions. If the user has access via AD Group membership, direct access, access through a SharePoint group or access through a SharePoint Group which has an AD group that the user is a member of (also supports multiple nested AD groups a user may be a member of), it will show up in the report that the user has access.

## Checking a User’s Permissions

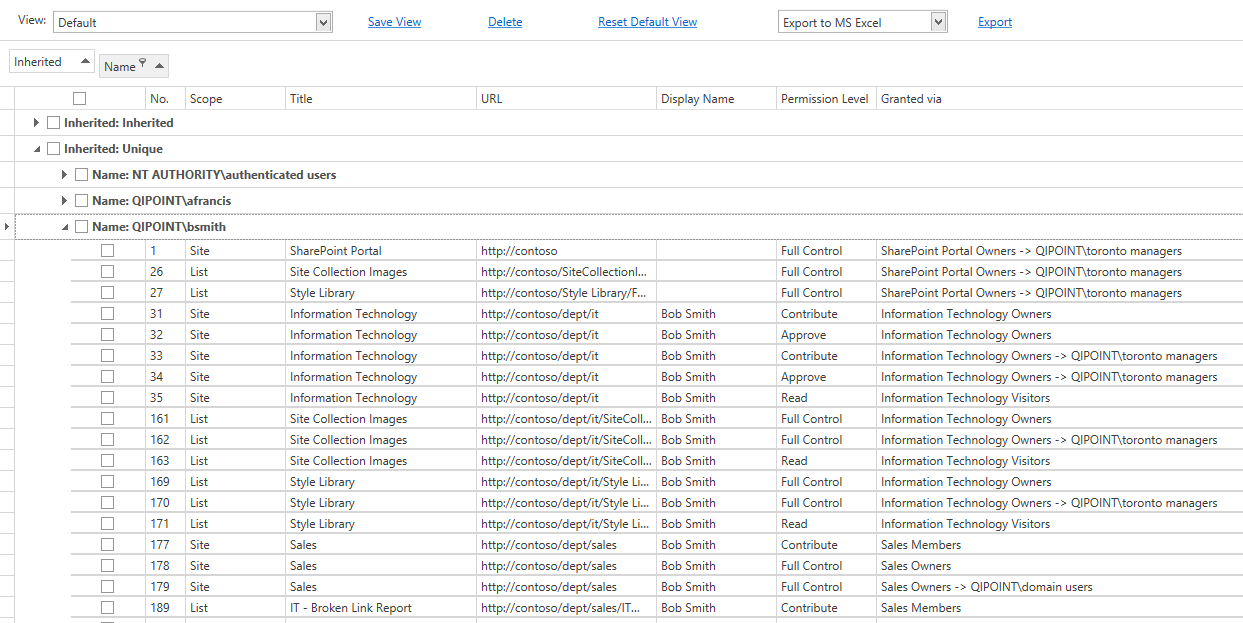
1. Open “SharePoint Essentials ToolkitTM”
2. Click on the “Permissions” tab at the top
3. Click on the “Check User Permissions” ribbon button
4. A new tab will appear called “Check Permissions”



1. The first section includes the job name and the credentials that will be used to check the user permissions. This should be an account with appropriate access to run the audit.
2. In the “Options” section, enter the user name of the account you want to audit, such as ‘DOMAIN\bsmith’, ‘Bob Smith’; or group name such as ‘Contoso Members’.
3. Select the sites that you want to include in the scan.
4. Click “Scan Now” button to start the audit.

Below is a sample report grouped by “Inherited Permissions” and then “Name”

TIP: You can easily sort and group columns to drill down and gather the information you need about the user’s permissions.



### Email and Export

See “**Report: Email and Export Options**” section

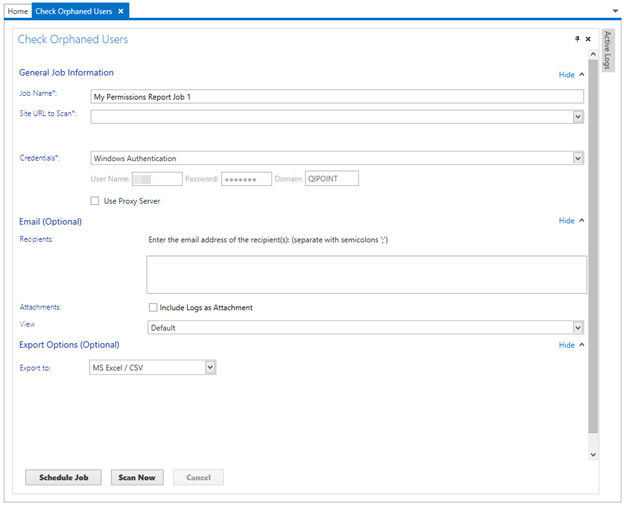
# Report: Orphaned User Accounts

## Summary

This report will help identify AD Accounts that have been used in SharePoint but later ‘disabled in Active Directory’. These accounts would still exist in SharePoint and are considered ‘Orphaned Users’.

## Checking for Orphaned Users

1. Open “SharePoint Essentials ToolkitTM”
2. Click on the “Permissions” tab at the top
3. Click on the “Check Orphaned Users” ribbon button
4. A new tab will appear called “Check Orphaned Users”



1. The first section includes the job name and the credentials that will be used to check for Orphaned User permissions. This should be an account with appropriate access to run the audit.
2. Enter the Site URL that you want to scan for Orphaned Users.
3. Click “Scan Now” button to start the audit.

# Report: Email and Export Options

### Email

Enter the email addresses for the users who you would like the report to be emailed to. Separate multiple email addresses with a semi-colon ‘;’. TIP: Enter <Contact Email> for the email address to use the ‘Contact Email’ specified for the site in the Home Page Dashboard.

**Include Logs as Attachment** - Optionally include the log files as an email attachment (they will be compressed/zipped).

### Export

This allows you to choose how to export the report when the scan job completes. You can use the default ‘MS Excel / CSV’ or select ‘SharePoint List’ to export the report to SharePoint.

#### Export to SharePoint List

**Site URL** - This is the target Site URL where the report (SharePoint List) will be created.

**List Name** – This is the List Title to be given to the List report.

**Auto Create List and Columns** – Check this option to automatically attempt to create the List and Columns. If the list already exists, it will attempt to create the list (only if the list does not exist) and recreate missing columns. If this option is UNCHECKED, it will not attempt to create the list or create the list columns. SharePoint Views that are created for the list are not overwritten when a report is generated/exported.

**Auto Append Site Title to Report** – This will automatically append the Site Title to the end of the List Name. For example, if the List Name is set to “List Permissions Report”, and the Site Title is ‘Information Technology’, the SharePoint List report that will be generated will be titled “List Permissions - Information Technology”

**NOTE:** If this job is targeting bulk sites (when creating reports against multiple site collections (by holding Shift/Ctrl from home page dashboard to create a report against multiple sites, see ***Batch Processing Multiple Site Collections***): If ‘Auto Append Site Title to Report’ is turned on, the Site Title will be appended to the end of the name of the report automatically and a report will be created for each site scanned (multiple SharePoint Lists, one per site). If ‘Auto Append Site Title to Report’ is turned off, all sites being scanned in the job will be merged into one single report (a single SharePoint List).

**Update Action** – Overwrite: This will first delete all SharePoint Items found (if list and items exist), then it will export the new report items to the list. The list will not be deleted so settings and views for the list remain intact. Append: This will append report items to the list and if there are existing list items, they will remain intact and will not be overwritten or changed.

# Opening the Report

Once a scan is complete you can open the report in several ways:

* + When a scan is complete, you will have a hyperlink on the top right (above the “Active Log”) that has links to each available Permissions report, they will open in a ‘grid view’.
  + Once you open a report in grid view, you can click “Export” to view the report in CSV/Excel format (the tool will also maintain the sorting, filtering and grouping) or export the report to a SharePoint list.
  + To access a permissions report that you ran against a site, you can right click on the site from the Home Page Dashboard, and select View Reports – Permissions Report
  + All Audits: From the “Permissions” ribbon tab, click on one of the reports you wish to view, there are 7 types of base ‘global’ audit reports you may further customize:
    - “All Site Permissions”: This report combines all existing reports into one view. This will show all site permission objects across farms, web applications, site collections and sites (from reports that have been generated).
    - “All List Permissions”: This report combines all existing reports into one view. This will show all list permission objects across farms, web applications, site collections and sites (from reports that have been generated).
    - “All User Permissions”: This report combines all existing reports into one view. This will show all users permissions granted across farms, web applications, site collections and sites (from reports that have been generated). These individual user audit reports are created when you used the “Check User Permissions” ribbon button to create a user audit report.
    - “All Unique Item Permissions”: This report contains a report that shows all of the unique item permissions given across all farms and sites (from reports that have been generated).
  + To view all MS Excel reports: from the ribbon, click on the “Home” tab, then click on “Reports and Logs”, windows explorer will open with the CSV reports and log files
    - Alternatively, you can manually navigate to this path. Open Windows Explorer and navigate to the path where the reports are stored (check “Settings”), the default location is in the user’s My Documents folder under “QIPoint\Reports”

# Editing Permissions

To edit permissions for one or more sites, you first need to run a report on those sites.

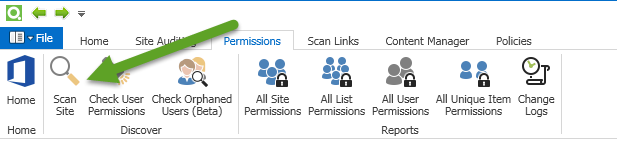
You can modify permissions in 2 ways:

1. SharePoint: Right click on the report row that you need to modify, then click Open Item Permissions. From here you can remove/modify/validate permissions for that report item
2. Within the Tool: Select the report records to modify by selecting left most column. Right click on a selected row and select “Edit Permissions”. A window will appear to modify the selected permissions.

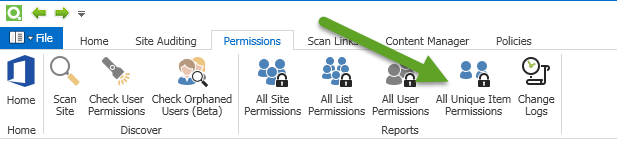
Below is an example of removing Item and Folder level permissions for specific users on a schedule using the tool:

## How to schedule removal of User Accounts (from Site/List or Item Level)

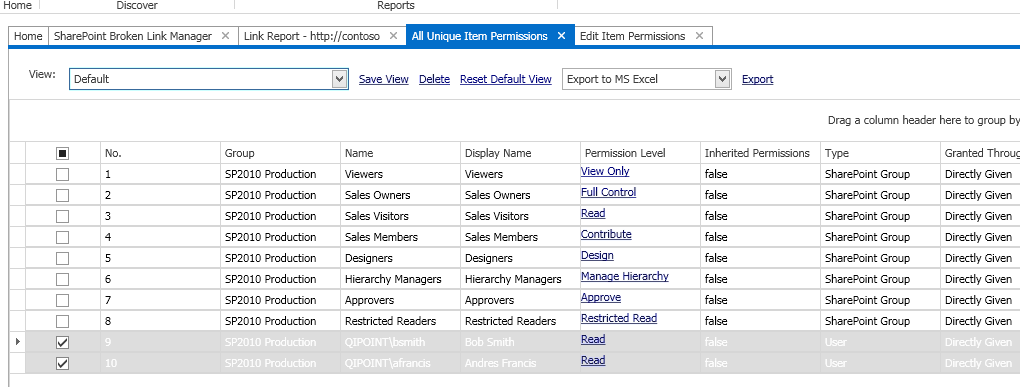
1. First you need to create a Permissions Report



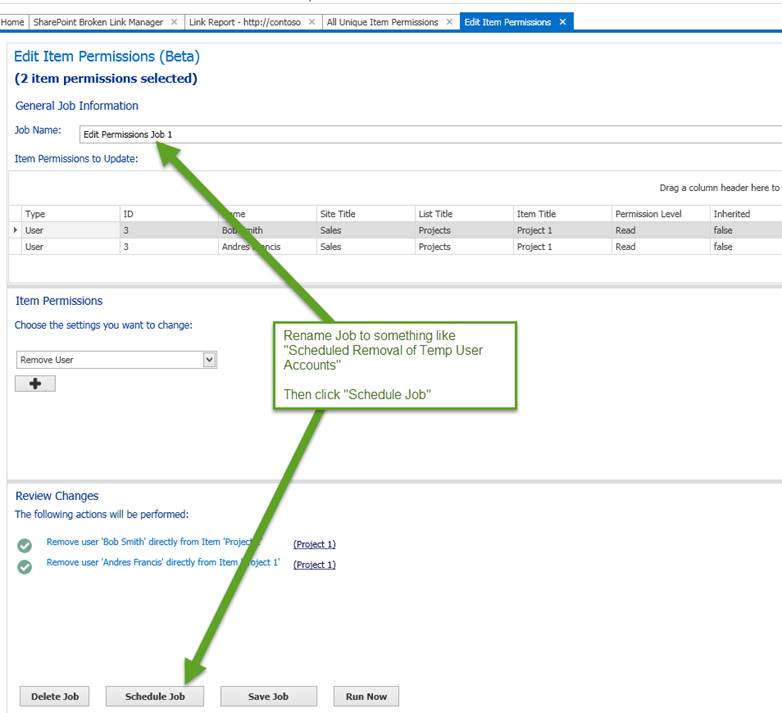
1. After that is complete, click “All Unique Item Permissions” from Permissions tab



1. Select the users you want to schedule the account removal (TIP: You can group by ‘Access Type’ and ‘Item Title’ to make it easier to view)



1. Then select option to remove the user(s)



1. Click Home (tab) -> Scheduled Jobs, and you should see the scheduled job created to remove the selected user accounts.
2. Make sure the scheduler service is running (Windows Service called “QIPoint Essentials Service”).



# Scheduling Scan Jobs (Enterprise version only)

This product includes a built in scheduler (Enterprise version only) which allows you to scan sites on a schedule. Scheduled jobs run faster than jobs manually run as they do not have to write logs to the UI (user interface).

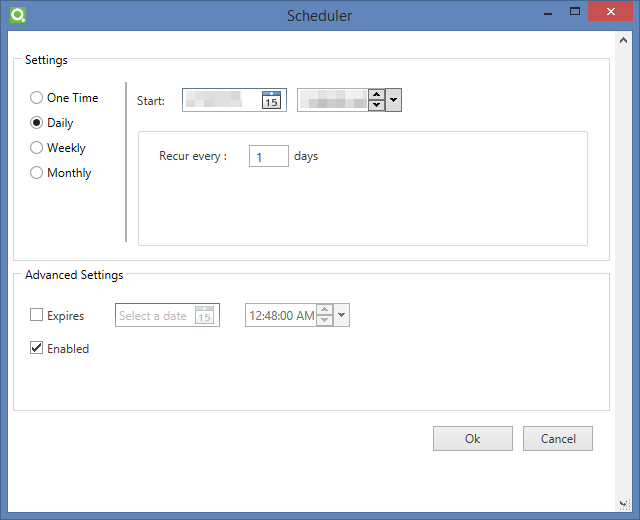
**TIP:** Ensure the “QIPoint Essentials Service” (Windows Service) is running before trying to schedule a job. Ensure the user account used to run the service has ‘Modify’ permission on folder C:\ProgramData\QIPoint as this is where the scheduler job information is stored.

## Schedule a Job

Once you complete the Scan Options page, click the “Schedule Job” button once ready to schedule this job. A window will appear to set the date, time and recurrence of this scan job.



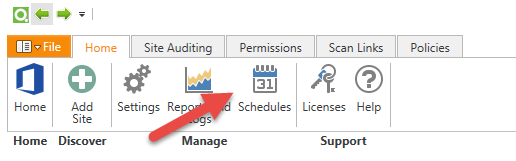
NOTE: You must use “Windows Authentication (Custom)” instead of “Windows Authentication” in order to save the credentials with the job. Passwords are encrypted.

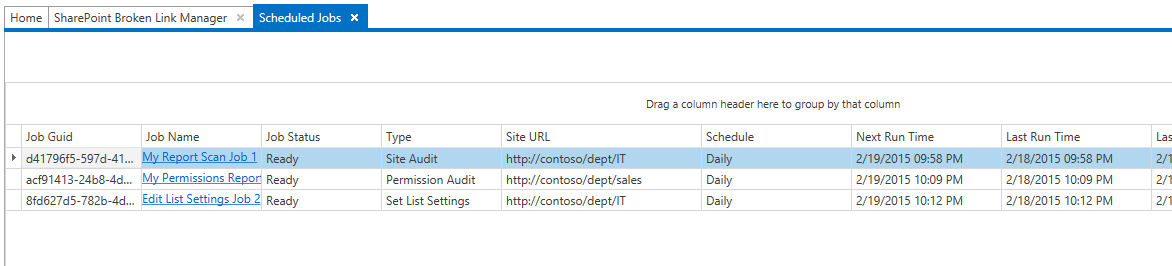


Select the schedule and specific options and click OK to save the scheduled job.

## Viewing & Managing Scheduled Jobs

You can view all scheduled jobs and their status’ by clicking on “Scheduled Jobs” from the Home page ribbon.





From here you can view reports, logs, execute the job, modify or delete scheduled jobs.

NOTE: Only applicable reports and logs will be shown.



# Licensing

## Components

The SharePoint Essentials ToolkitTM by QIPoint may have multiple components activated to provide more functionality.

To view what components are installed, on the ribbon, click Home -> Licenses.

## Changing the license type of a component

1. Start “SharePoint Essentials ToolkitTM”
2. From the “Home” Ribbon tab, click on “Licenses”
3. If you are using a Trial Version:
   * Click on “Activate Now” beside the product you want to changing licenses for

If you are using a Licensed Version:

* + Click on “Change License” beside the product you want to changing licenses for

1. Select the **Version** of the application component you would like to activate, example, change to “Enterprise” for the Enterprise version.
2. If you have a paid license key, enter it in the “License Key” text box
3. Click Activate
4. Close any open tabs in order for the new licensing options to become available (or hidden if downgrading the license). The new options will appear once the tab is reloaded. You do not need to shut down the application.

## Obtaining a License

There are three ways you can purchase a license

1. Online: visit <http://www.qipoint.com/>
2. Call us at 1-855-747-6468
3. Email us at [sales@qipoint.com](mailto:sales@qipoint.com)

You may place your order and receive a license key with a PO# or Credit Card

## Transferring a License

You may need to transfer the license if the machine was lost, stolen, re-formatted, or if you would like to assign a license to another user. Contact us to obtain a new license activation key at [support@qipoint.com](mailto:support@qipoint.com).

# Customizing Permission Reports

You can generate many customized reports, below are some of the standard reports that are created, which can then be further customized and saved by the tool:

## Site Permissions Report

#### Summary

The “Site Permissions Report” provides a report on SharePoint site permission objects. It can be used to find what sites a particular user/group has been granted access to in the ‘Site Permissions’ pages.

#### Example Metadata Captured in Audit

* Group / Users
* Ids of group/user
* Permission levels
* If site is using Inherited permissions
* More…

#### Usage: Example Custom Reports

An example of some custom reports could be

* “John Doe permissions granted directly on all sites”
* “Where ‘HR Group 1’ has Project Site READ permission levels”
* “All Users who are given direct access to sites – which need to be removed or added to groups”
* “Sub sites that are using Custom Permission Levels”
* …

## List Permissions Report

### Summary

The “List Permissions Report” provides a report on SharePoint lists permissions (across a single site or multiple site collections). It can be used to find what lists a particular user/group has been granted access to in the List Permissions pages.

### Sample Reports

#### Permission Info Captured in Audit

* Group / Users
* Ids of group/user
* Permission levels
* If site is using Inherited permissions
* List visible or hidden
* Parent Site
* More…

#### Usage: Example Custom Reports

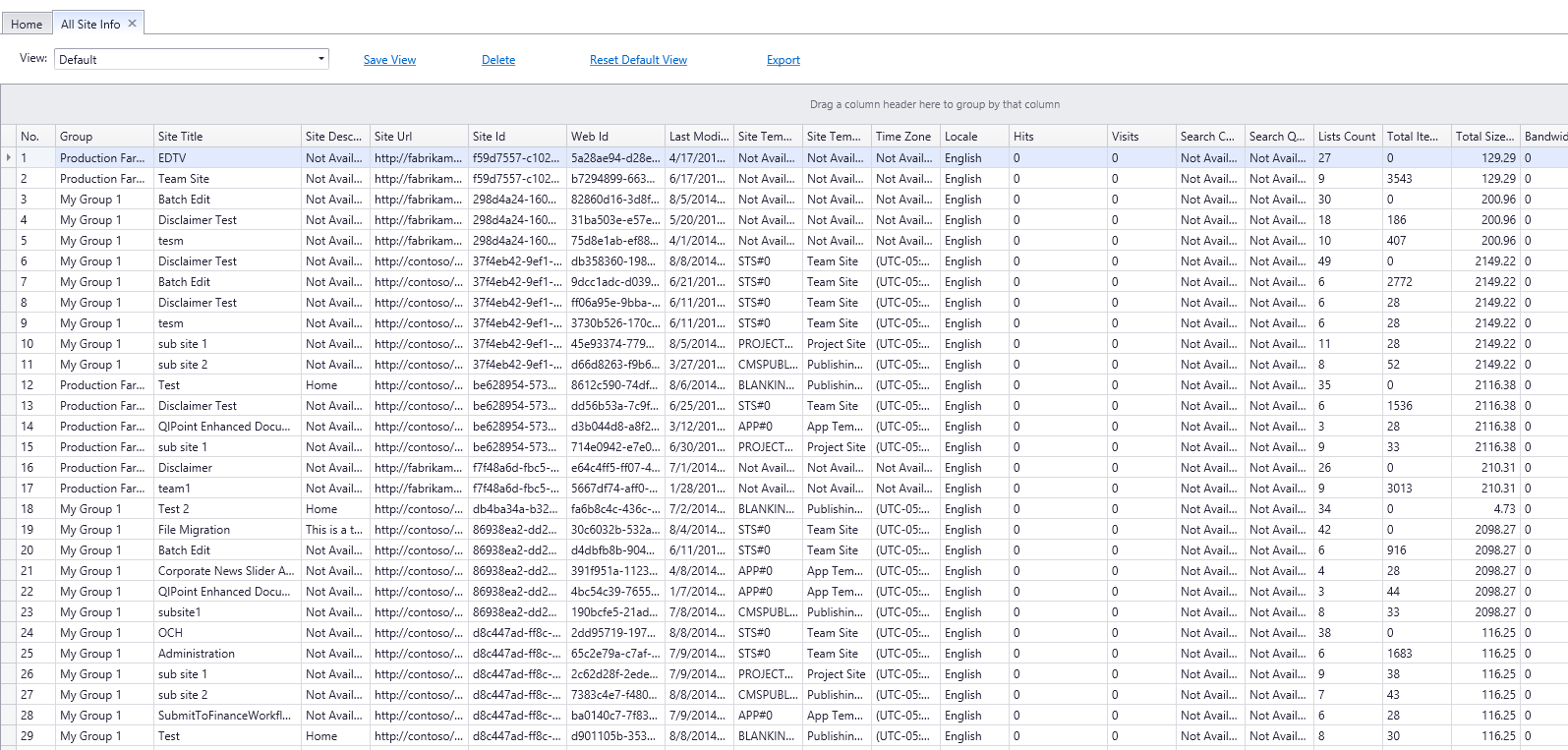
An example of some custom reports could be

* “Find where John Doe is granted direct access and the permission level used in all lists”
* “Identify which lists ‘HR Group 1’ has READ permission levels”
* “All Users who are given direct access to lists – which need to be removed or added to groups”
* “Lists that are using Custom Permission Levels”
* …

### Grid View Report

All reports can be viewed in a ‘Grid View’, see screenshot below:

Example Grid View:



### Customizing the Report

You can filter, sort, search and group the results from the scan job.

### Filtering

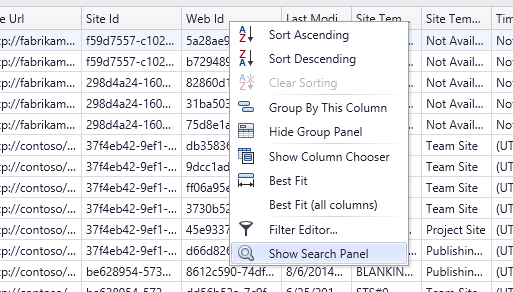
To filter the data based on a field, put your mouse over the column header that you want to filter by. You should see a filter icon, select it and choose the values you only want to have shown in the grid

### Advanced Filtering

To filter the data based on a field using advanced criteria, right click on the column header and select “Filter Editor”. You can now add criteria to filter the results

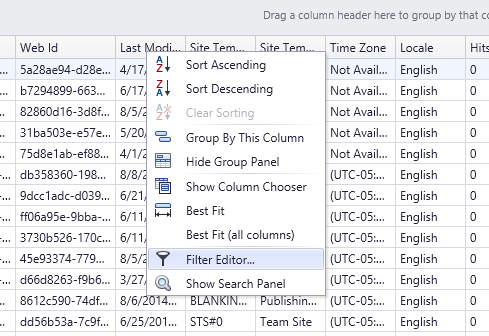
### Searching within the Report

Right Click on any column header and select “Show Search Panel”. The search panel will appear and you can enter any value to search the grid, results will be highlighted

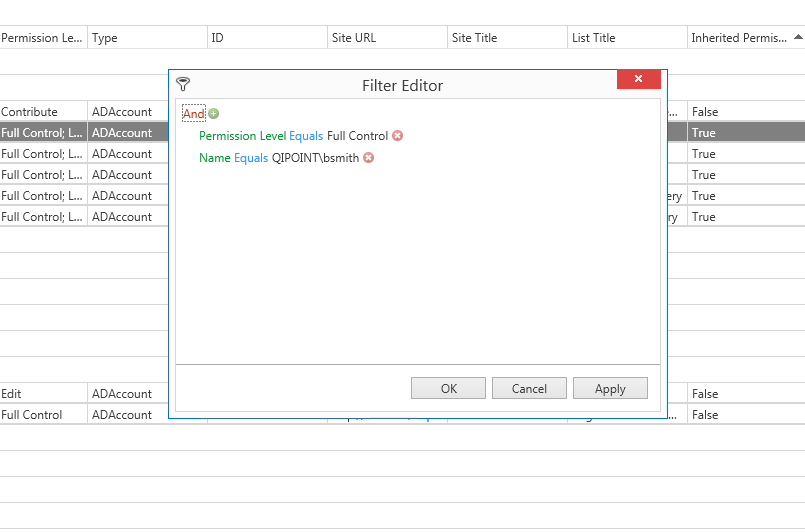


### Filtering Queries

You may also filter the report by using queries. Right click the column header and select “Filter Editor” to add criteria to filter the results

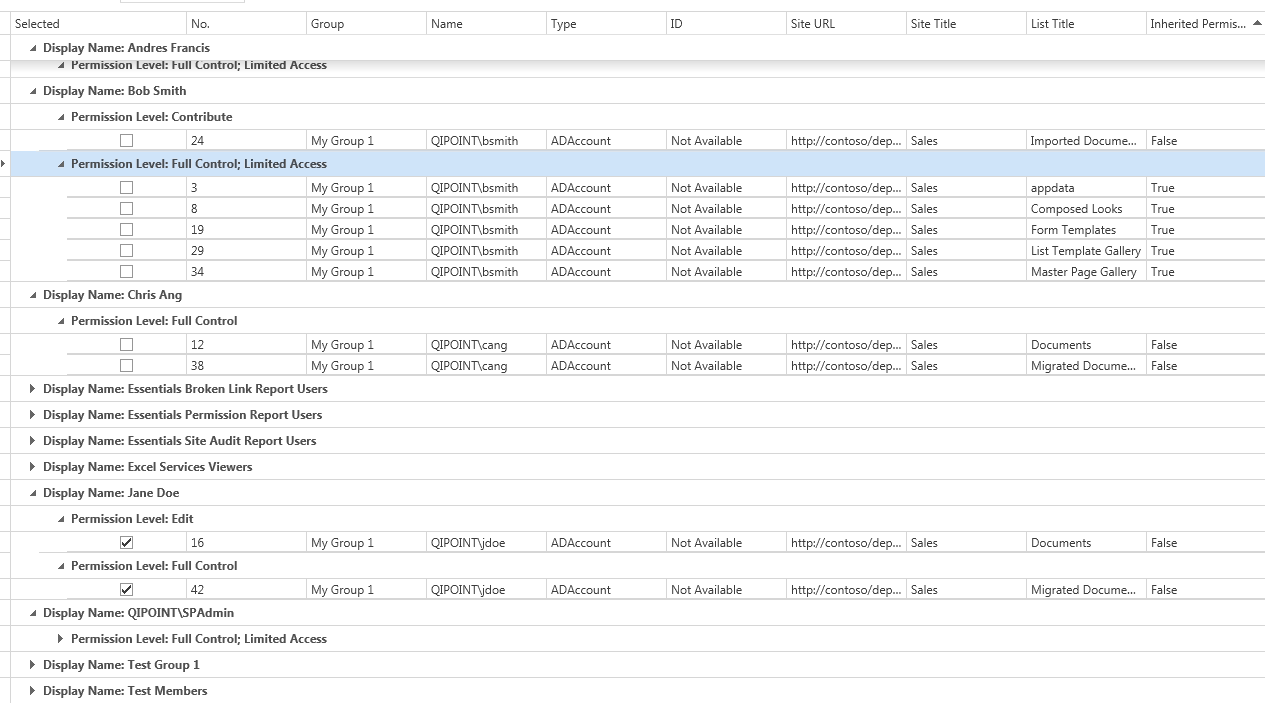


Add a single filter criteria or multiple filters/logic, including grouping IF/AND/OR statements



### Grouping

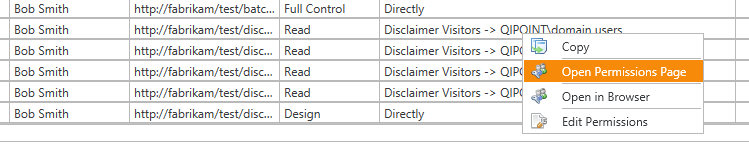
To group the results, drag the column header of the field you want to group by to the top of the results panel. You can also drag multiple panels and rearrange the group ordering by dragging columns left and right of each other



# Editing User / Group Permissions

## Manually Updating User / Group Permissions

If the user finds a Site or List with user or group permissions they need to correct, they may right click on the report item in Grid View, and click “Open Site Permissions”, “Open List Permissions” or “Open Permissions Page” (depending on the report being viewed) to manually update the setting/permission for that item in SharePoint.

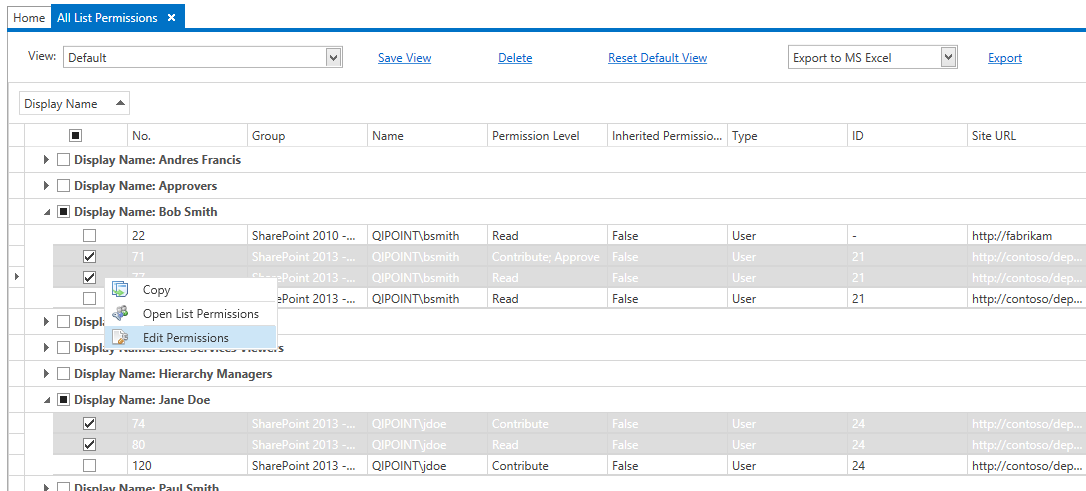


## Automatically Updating User / Group Permissions

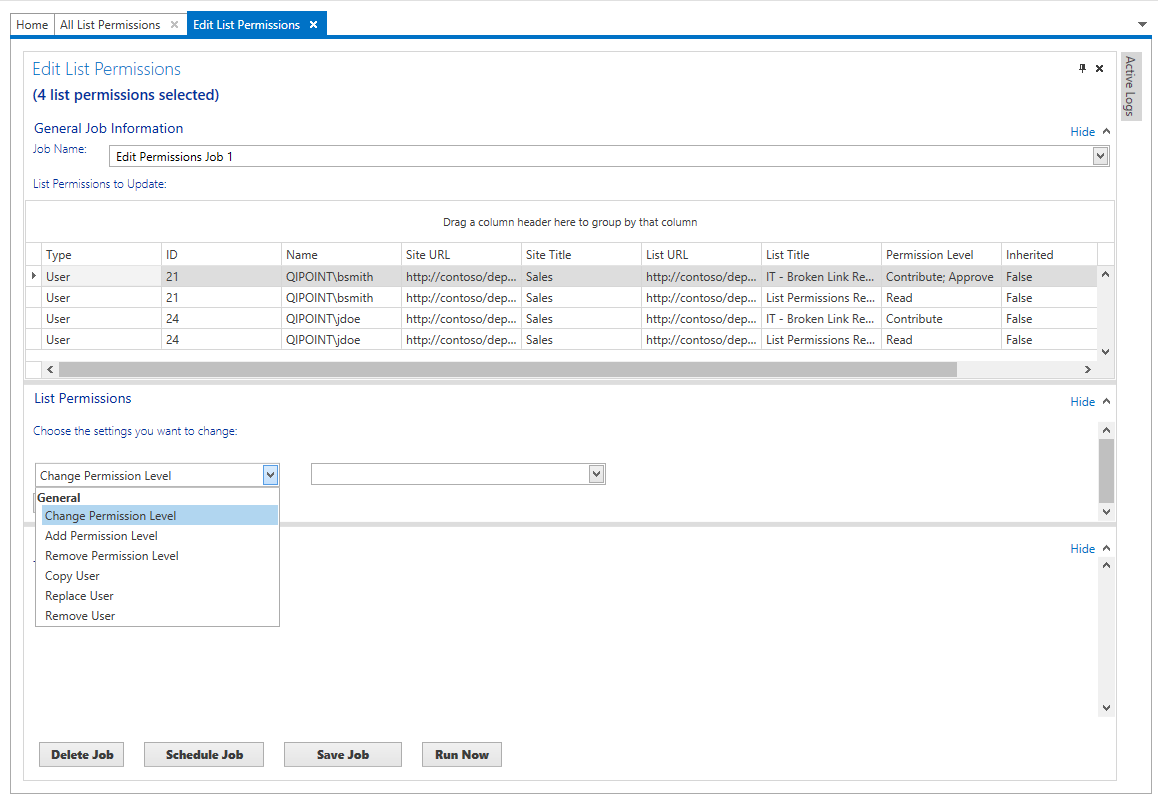
If the user finds a Site or List with permissions that they need to correct:

* From the grid view report Select the permissions you wish to modify
* Right click, and select “Edit Permissions”

**Example:** Below we have selected 4 permission objects where we want to change Bob Smith and Jane Doe’s permission/access. These permission objects can be from the same farm/web application/site collection or different ones.



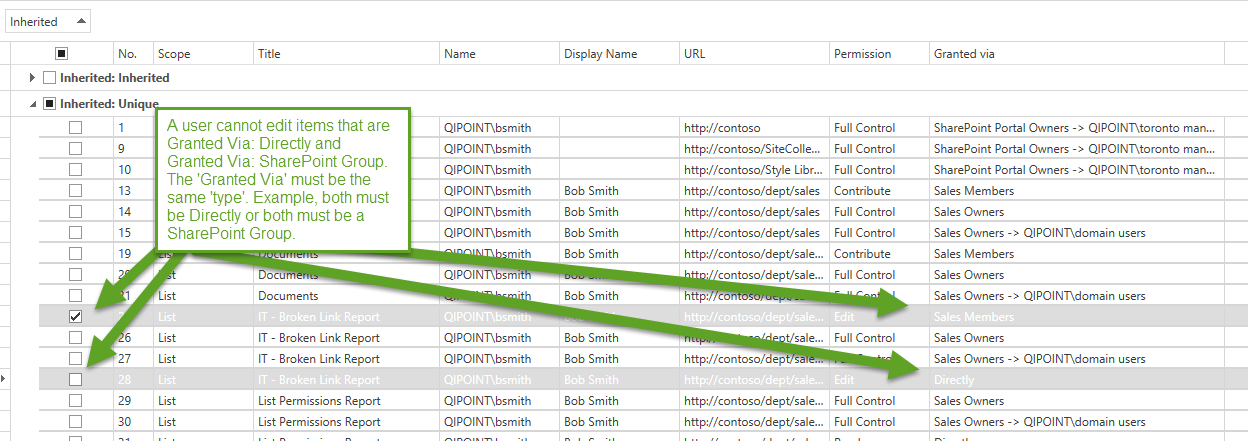
* The Edit Permissions window will open. This is where you can: modify the selected objects permissions, copy the permissions to another user/group, replace the user/group, or just remove access.



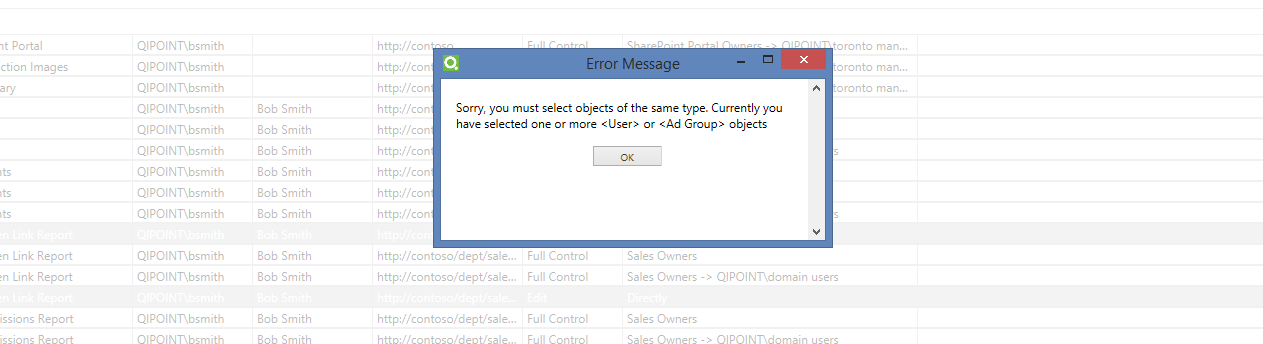
**NOTE**

* Only non-Inherited permissions can be modified. If permissions are inherited and you wish to make a change, you will need to modify the parent object (the parent site or list it is inheriting from).
* In the ‘Check User Permissions’ report, you can only Edit objects that are of the same Permission type at ONE TIME (AD Account (directly) or SharePoint Group), see the column ‘Granted Via’.

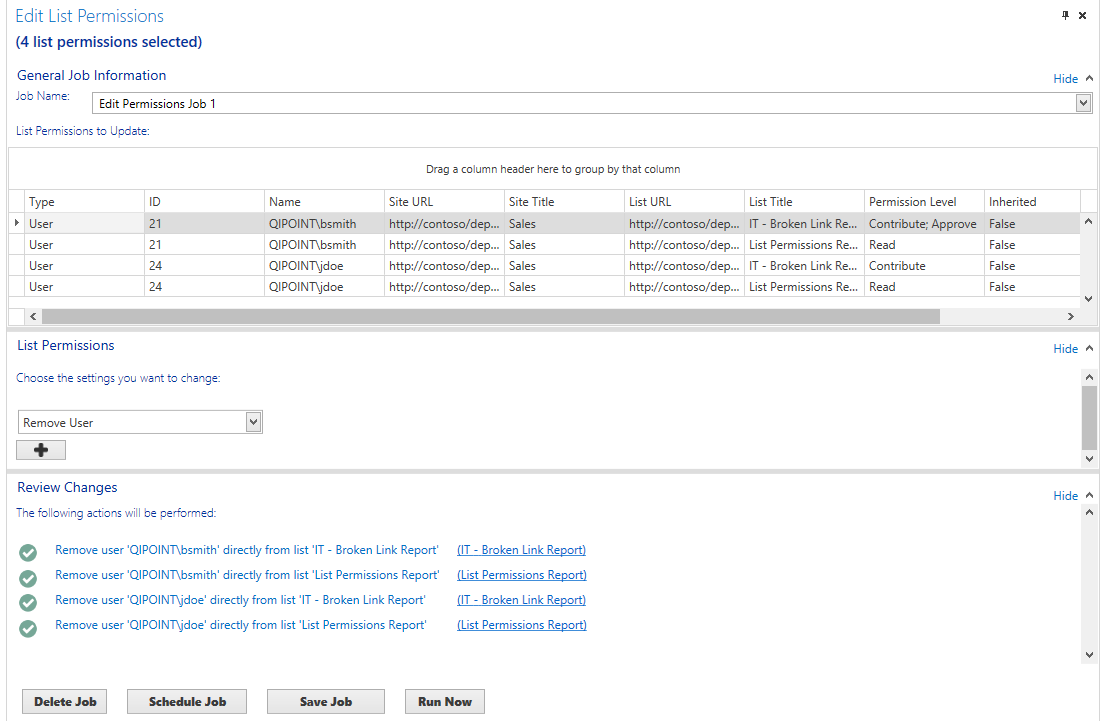
For example, if you have a report with permissions granted for Bob Smith, and one list shows ‘Granted Via: directly’ (which indicates the User’s permission was added ‘directly’ to the list) and another list shows ‘Granted Via: SharePoint Portal Members’ (where the user was granted access by adding the user to the SharePoint Group ‘SharePoint Portal Members’), you cannot update both at the same time. This is because some changes to a User is different than from a SharePoint Group, such as removing a User’s permissions directly from the list vs removing a User’s permissions from the list by removing them from a SharePoint Group. You will get prompted when you try to do this and advise you that you cannot edit items that are not the same type.



This message will appear advising user they must be of the same type:



Below is an example of removing the 4 permission settings from the 2 lists:



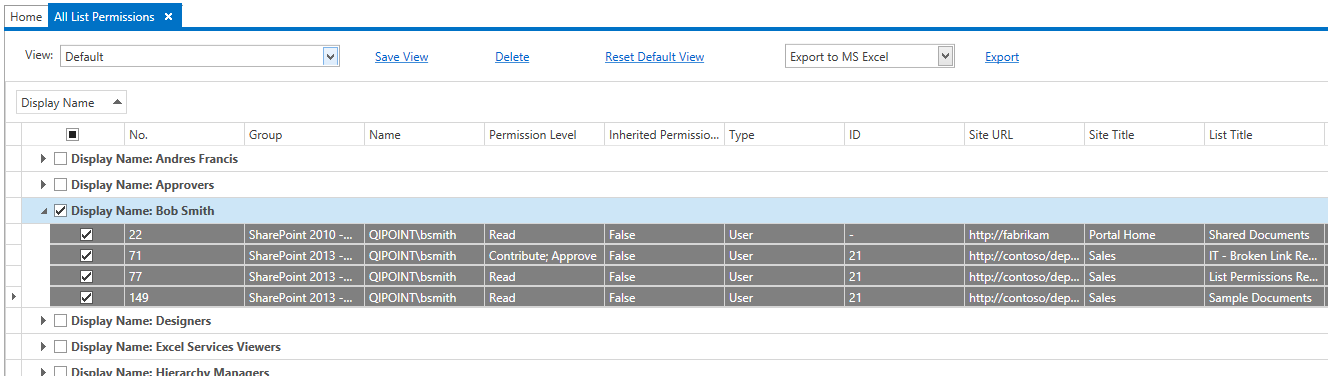
# Permission Templates – “Save Job”

You can set up a ‘template’ by “Saving a Job” based on the target Permission Objects you want to have set.

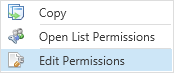
To do this:

1. Open a report (such as a Site, List, Unique Item or User report)
2. Select the permission objects you want to add to the ‘template’

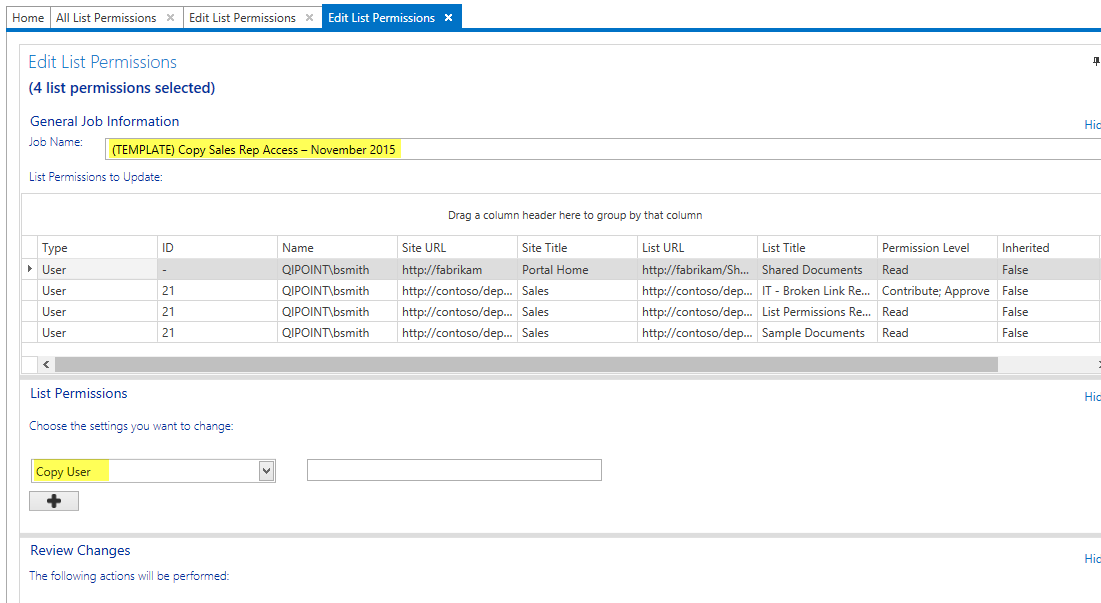
For example, if a user needs to grant access to other users based on Bob Smiths access (perhaps he is a Sales Rep and I often need to duplicate his access to others), I would select his permission objects as done below: (in this simple example Bob Smith only has unique access to 4 lists)



1. Right click and select “Edit Permissions”

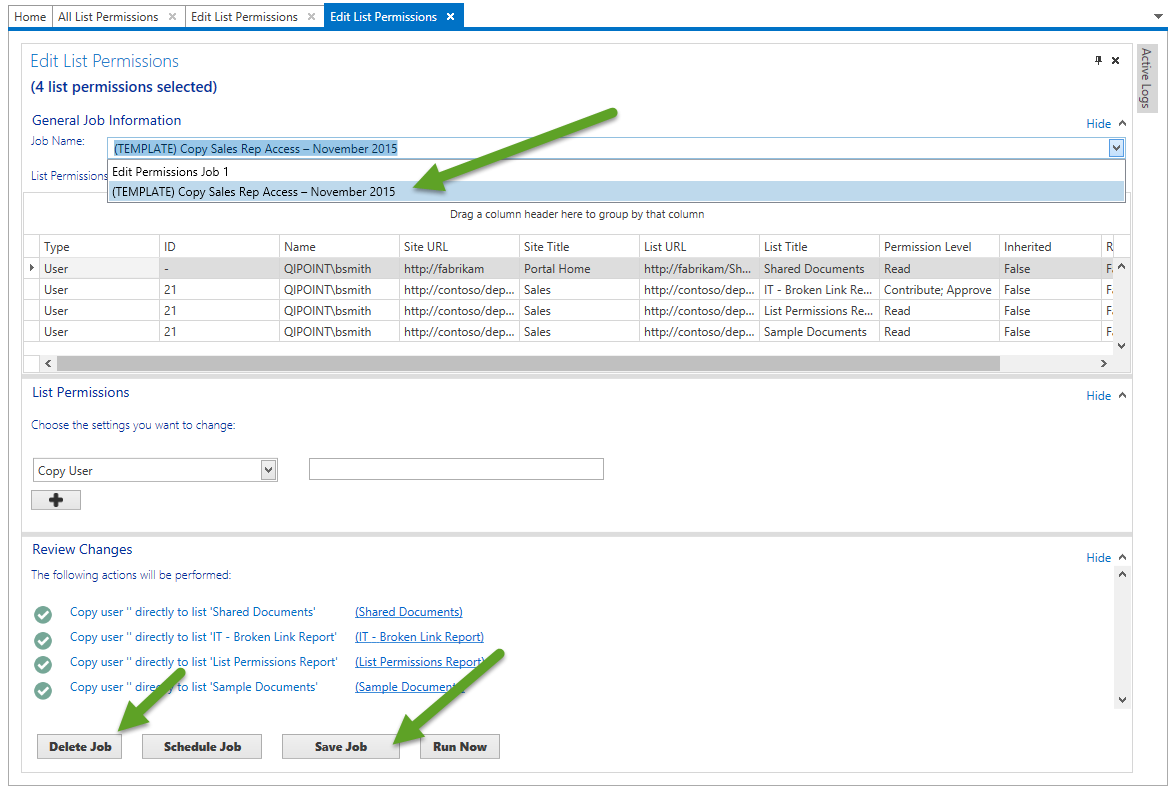


1. The Edit List Permissions window will open (or whichever appropriate window based on the permission template being created, such as Edit Site Permissions)
2. Enter a unique Job Name for the ‘template’, such as “(TEMPLATE) Copy Sales Rep Access – November 2015”



1. Under List Permissions section, select “Copy User” (or appropriate action for the template)
2. Enter the user to be copied or leave it blank in the template and click “Save Job” button
3. The ‘template’ will now be saved and can be reused later to apply the permissions to another user

The template can be modified and re-saved or deleted by clicking “Delete Job” while it is selected in the “Job Name” drop down list.



# Report Archive

When a report is created and there is a report that already exists for that scan (this occurs if it is the same site URL that is scanned and on the same day), the old report (and the related log file) will be renamed and moved to a folder called “Archive” in the same directory. The new report will then be created.

# Technical Support

If you need technical assistance, not to worry! We offer several ways to get in touch with our support team.

**Email:** [support@qipoint.com](mailto:support@qipoint.com) (Average response time is 3-8hrs)

**Phone:** 917-633-5998 opt. 1

**Online Support Ticket System:** <http://support@qipoint.com>

We are here to help! Even if you are using the free version of our tools!

# Version Comparison

|  |  |  |
| --- | --- | --- |
| Feature | Professional | Enterprise |
| Scan SharePoint 2010 |  |  |
| Scan SharePoint 2013 |  |  |
| Scan Office 365 |  |  |
| Scan SharePoint Sites |  |  |
| Searching within Report |  |  |
| Querying results in the Report |  |  |
| Report in customizable grid |  |  |
| Report Site, List and Item level Permissions |  |  |
| Report Permissions across Farms & Site Collections |  |  |
| Include User AD Group Permission membership |  |  |
| Nested AD Group permissions |  |  |
| Hide Limited Access in Reports |  |  |
| Report Specific User or Group Permissions |  |  |
| Export to CSV / MS Excel |  |  |
| Grouping of Scan Results in grid |  |  |
| Scan Entire Site Collection in single job |  |  |
| Edit Permission Objects in Bulk |  |  |
| Email results automatically to users |  |  |
| Schedule Scan Jobs & Report Generation |  |  |
| Export Reports to SharePoint List |  |  |