|  |
| --- |
|  |
| SharePoint Permissions Manager™ |
| User Manual |
|  |
|  |
| **8/17/2017** |

|  |
| --- |
|  |

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

Table of Contents

[Introduction 4](#_Toc490735170)

[Installation & Minimum Requirements 5](#_Toc490735171)

[IMPORTANT: This program does not need to be installed on a SharePoint Server. 5](#_Toc490735172)

[Minimum Hardware Recommendations 5](#_Toc490735173)

[Supported SharePoint Versions 6](#_Toc490735174)

[.NET Framework Required 6](#_Toc490735175)

[Local Machine & Windows System Permissions Required 8](#_Toc490735176)

[Anti-Virus, Offline Sync Folders (i.e. Google Drive, OneDrive, Drop Box, etc) and Performance 8](#_Toc490735177)

[SharePoint User Permissions Required 9](#_Toc490735178)

[Full Permissions Reporting 9](#_Toc490735179)

[Limited Permissions Reporting (‘Least Privileged’) 9](#_Toc490735180)

[Office 365 Accounts 10](#_Toc490735181)

[Getting Started 11](#_Toc490735182)

[Quick Overview 12](#_Toc490735183)

[Discover 12](#_Toc490735184)

[Scanning Multiple Sites at Once 14](#_Toc490735185)

[Reports 14](#_Toc490735186)

[Limitations 18](#_Toc490735187)

[Basic Permissions Reports 21](#_Toc490735188)

[What is a Basic Permissions Report? 21](#_Toc490735189)

[How to Create a Basic Permissions Report 21](#_Toc490735190)

[Check User Permissions Reports 35](#_Toc490735191)

[How to Create a User Permissions Report 35](#_Toc490735192)

[Inclusion Rules (Optional) 39](#_Toc490735193)

[Exclusion Rules (Optional) 39](#_Toc490735194)

[NOTE: Inclusion/Exclusion Rules: 39](#_Toc490735195)

[Export Options 40](#_Toc490735196)

[Check Orphaned Users 43](#_Toc490735197)

[How to Create an Orphaned Users Report 43](#_Toc490735198)

[Logs 46](#_Toc490735199)

[How to Interpret the Reports 48](#_Toc490735200)

[Interpreting the Reports 48](#_Toc490735201)

[Opening the Report 48](#_Toc490735202)

[Merged Reports 61](#_Toc490735203)

[Customizing the Report 63](#_Toc490735204)

[Filtering 63](#_Toc490735205)

[Advanced Filtering 63](#_Toc490735206)

[Searching within the Report 64](#_Toc490735207)

[Grouping 65](#_Toc490735208)

[Views 66](#_Toc490735209)

[Export 67](#_Toc490735210)

[Permission Templates – “Save Job” 68](#_Toc490735211)

[Manage 71](#_Toc490735212)

[Editing Permissions 71](#_Toc490735213)

[Manually Updating User / Group Permissions 71](#_Toc490735214)

[Automatically Updating User / Group Permissions 71](#_Toc490735215)

[How to schedule removal of User Accounts (from Site, List or Item Level) 74](#_Toc490735216)

[Scheduling Jobs 77](#_Toc490735217)

[Schedule a Job 77](#_Toc490735218)

[List of Scheduled Jobs 79](#_Toc490735219)

[Scheduled Job Logs and Reports 80](#_Toc490735220)

[Report Archive 81](#_Toc490735221)

[Licensing 82](#_Toc490735222)

[Components 82](#_Toc490735223)

[Changing the license type of a component 82](#_Toc490735224)

[Obtaining a License 82](#_Toc490735225)

[Transferring a License 82](#_Toc490735226)

[Technical Support 83](#_Toc490735227)

[Product Features 83](#_Toc490735228)

# 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 1GB available RAM. Recommended 2GB available RAM or higher

We recommend:

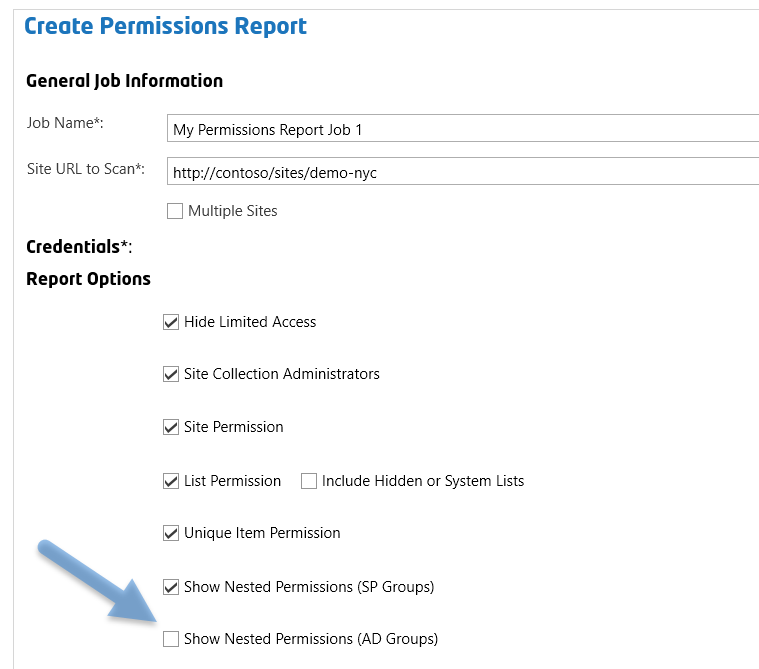
* At least 1GB of available RAM for jobs\* with less than 1,000 uniquely permissioned objects
* At least 2GB of available RAM for jobs\* with less than 5,000 uniquely permissioned objects
* At least 4GB of available RAM for jobs\* with less than 100,000 uniquely permissioned objects
* At least 6GB of available RAM for jobs\* with less than 500,000 uniquely permissioned objects

\*Jobs – includes all jobs being run at one time, such as multiple jobs in a schedule for one or more sites

**NOTE:** The tool caches SharePoint Groups and AD Group permissions to improve performance (vs. re-fetching all of this information multiple times for the same objects). However, the memory requirement may still vary depending on the number of unique permissions set on the sites. For sites with significantly more uniquely permissioned objects, they will require more RAM to be used to store the permission information for the reports. The figures above are just a general guideline to follow and actual RAM required may vary depending on the site being scanned and number of permission objects within them.

**“Show Nested Permissions (AD Groups)”**

This option is used to retrieve AD/Active Directory Objects (such as Users and Groups) nested within an Active Directory Security Group. For example, Marketing Managers may be a group within Marketing Users, both groups having a set of user members, enabling this option checks all groups within groups. In many organizations, this number (number of members) can be in tens of thousands, and in some cases 100K depending on the AD Group member count. If you enable this feature and find that the report hangs or is not completing, you may need to add more RAM or uncheck this option in the permission reports.



**Hard Disk:** 300MB 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 Online / 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
* Or have Full Control at Site (SPWeb) level

## Limited Permissions Reporting (‘Least Privileged’)

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 Site Collection Administrators report will also not be available with the permissions below.

**IMPORTANT:** The “Show Nested Permissions” options will not work with the permission level below. Therefore, users within SharePoint and AD Groups will not be visible in reports. If you need to report on nested permissions, the account used must have Full Control (shown in above section).

**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.

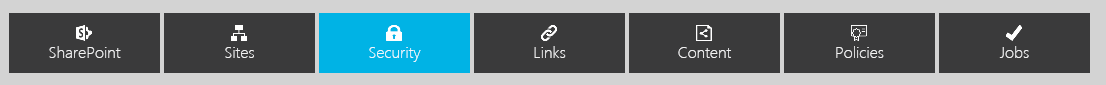
**Open -** Allows users to open a Web site, list, or folder in order to access items inside that container.

**NOTE: T**he above permission levels are required for each site you will be running a report for. If the report is being run for a subsite, the account running the tool will require Read permission on the root site. The account will require **Manage Permissions** permission level if the user would like to use the ‘Edit Permissions’ option in this component.

## 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.

# Getting Started

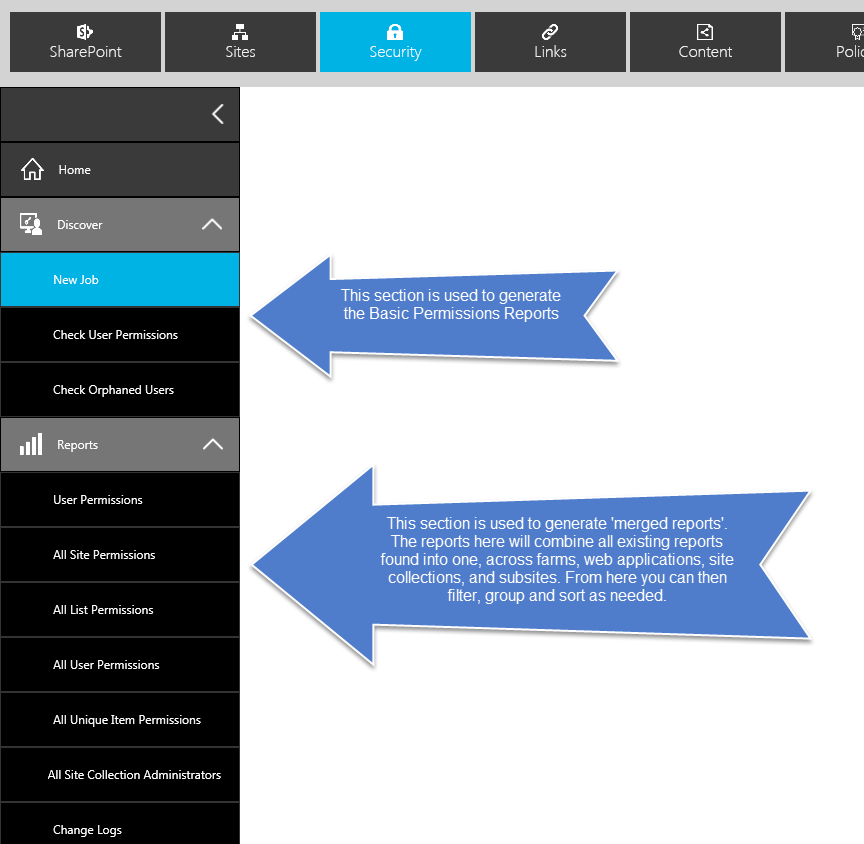


There are several types of security reports you can generate using this tool. They are listed below.

The tool works with the process: “Discover, Analyze, Manage”

## Quick Overview

The first thing you need to do, is to generate Basic Permission reports using the “Discover” section.



### Discover

This section in the Left Navigation allows you to generate new Basic Permissions Reports, listed below.

#### New Job - Basic Permissions Reports (Site)

This will create a new Permissions report for a given **SharePoint Site**. It will generate Site-level, List-level and Item-level permissions reports. See “[Basic Permissions Reports](#_Basic_Permissions_Reports)” below for more information.

#### Check User Permissions

This will create a new Permissions report for a given **User**. You will be prompted to select the user to report against, and all of the sites to check for this user’s access. It will generate a single report that includes all permissions for the user granted at the Site-level, List-level and Item-level. See “[Check User Permissions Reports](#_Check_User_Permissions)” below for more information.

#### Check Orphaned Users

This will create a new Permissions report for to display all **Disabled or Missing Users** in the SharePoint site. It will generate a single report that includes all Orphaned Users found at the Site-level, List-level and Item-level. See “[Check Orphaned Users Reports](#_Orphaned_User_Accounts)” below for more information.

### Scanning Multiple Sites at Once

To create jobs for multiple sites and subsites, see the “SharePoint Essentials Toolkit User Guide” under the section “Batch Processing Jobs for Multiple Sites”.

### Reports

This section in the Left Navigation allows you to build reports based on the Basic Permissions reports above. For example, the All List Permissions report will automatically merge all list permissions reports into one, so that you can filter, sort and group columns to view all lists that a specific user has access to across multiple sites, site collections, web applications and even farms.

#### All Site Permissions

This will create a merged Site Permissions report. This will display all Site Level permissions for all SharePoint Sites that you have created a Basic Permissions Report (for the sites you manage).

For example, you can schedule jobs for each of the SharePoint Sites that you manage, then view access for specific users or groups across all of those sites using this single ‘merged’ report.

#### All List Permissions

This will create a merged Check User Permissions report. This will display all List Level permissions for all SharePoint Sites that you have Basic Permissions Report (for the sites you manage).

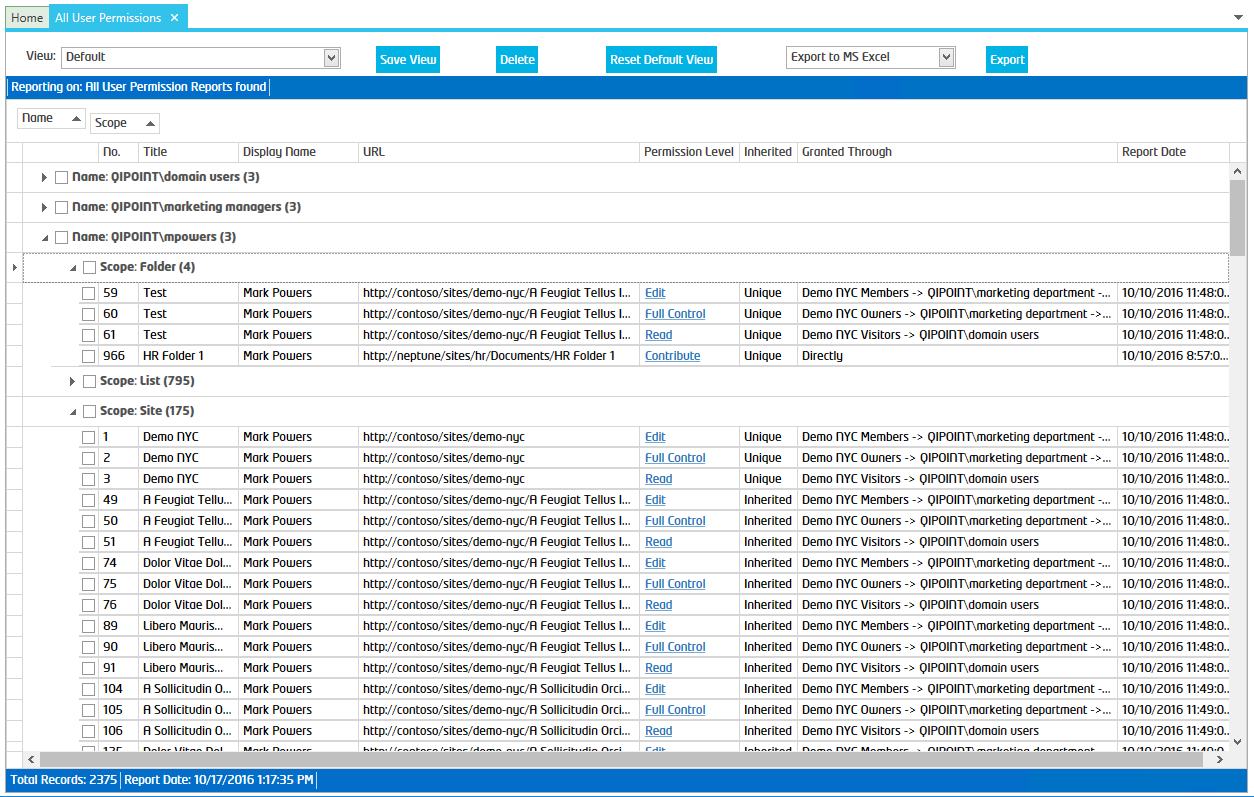
For example, you can schedule jobs for each of the SharePoint Sites that you manage, then view access for specific users or groups across all lists using this single ‘merged’ report.

#### All User Permissions

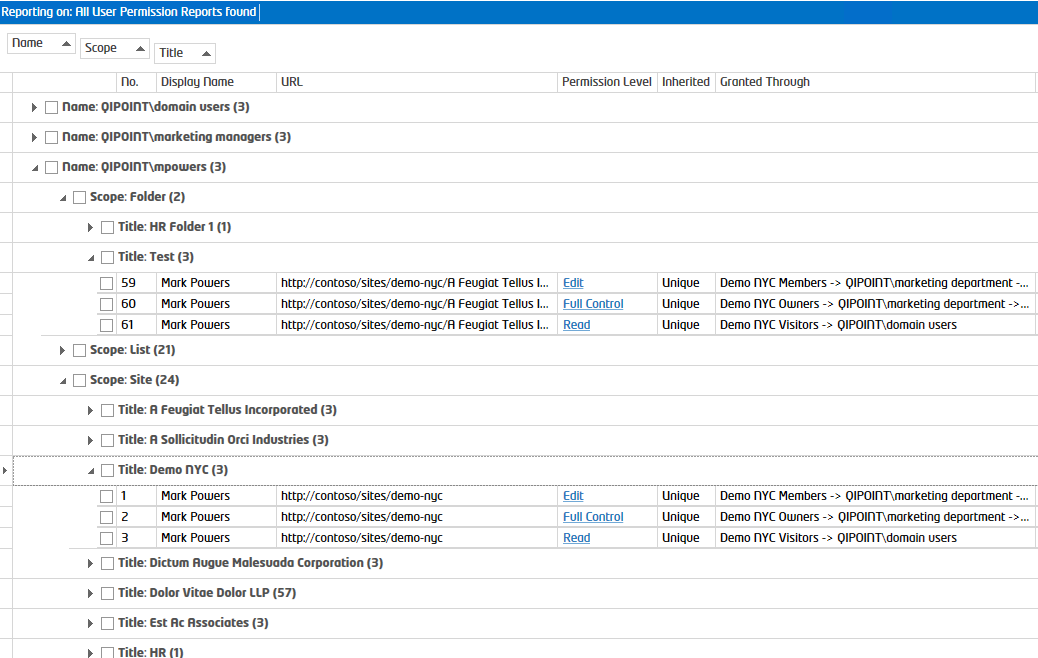
This will create a merged Check User Permissions report. This will display all permissions for the Users that you have “Checked Permissions” for.

For example, you can run a job on a schedule for all members of your team, and use this report to view the permissions granted for each of them and where they have access for the sites you manage.

Example Below:



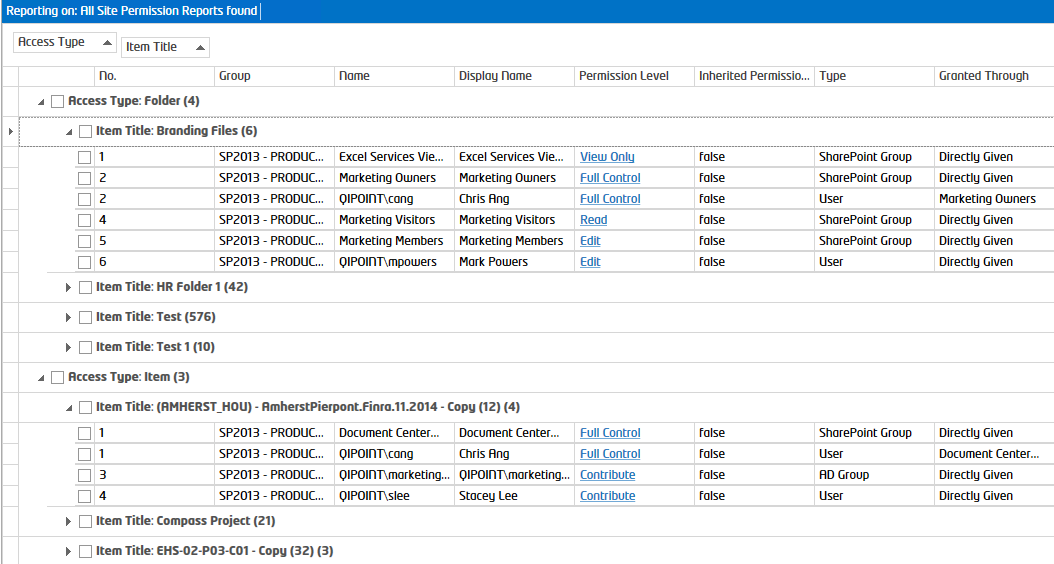
Another View of the same report:



#### All Unique Item Permissions

This will create a merged Unique Item Permissions report. This will display all Item Level permissions for SharePoint Sites that you have created a Unique Item Permissions report (for the sites you manage).

For example, you can schedule jobs for each of the SharePoint Sites that you manage, then view access for specific users or groups across all of those sites using this single ‘merged’ report.



### Limitations

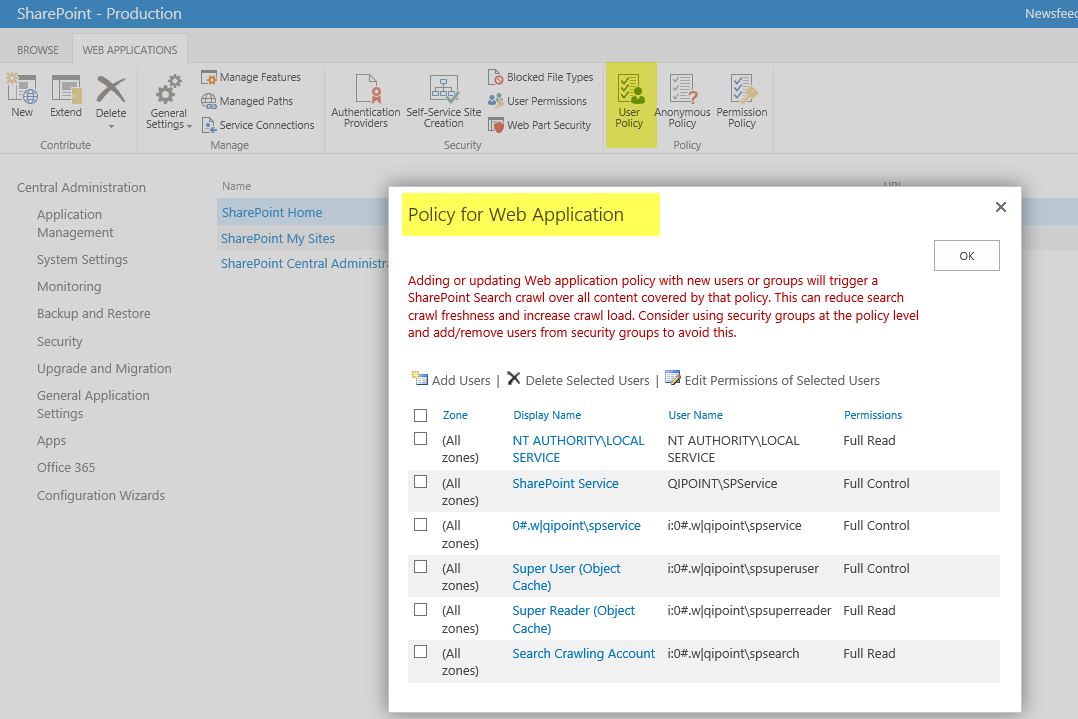
**IMPORTANT NOTES:**

* Permissions shown in the reports do NOT show Web Application User Policies applied. Farm, Search and other accounts that are specified in the Web Application User policy are not checked for permission access or shown in the reports. The reports generated by this tool cover Site Collection, Site, List, Folder and Item level, but not the Web Application Level. Normally, permissions at the Web Application level do not change frequently, and can be viewed in one spot in Central Administration. See below for more help on finding these permissions.
* If the account/groups ‘Everyone’ or ‘NT Authority\Authenticated Users’ is found, and ‘Show Nested Permission (AD Groups)’ is selected, the tool will show all active (not disabled) AD Accounts where the object class is User or Person. It does not include Local Machine Accounts which could have access through these permission levels.
* (SharePoint Online only) Permissions shown in the reports do NOT include permissions of users within SPO Groups that are defined in the Office 365 Groups in SharePoint Administration panel. These nested SPO permissions will be included in a future update.

Web Application User Policy Permissions

The toolkit is designed for Site Owners and Site Collection Administrators who may not have access to view permissions at the Web Application level.

Below is where you may check for permissions at this level: (Central Administration->Application Management->Manage Web Applications)



Office 365 / SharePoint Online SPO Groups

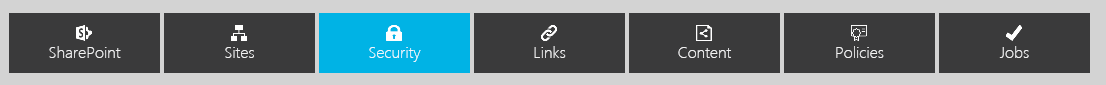
**IMPORTANT:** Permissions shown in the reports do NOT include permissions of users within SPO Groups that are defined in the Office 365 Groups in SharePoint Administration panel. These nested SPO permissions will be included in a future (free) update included with license.

## Basic Permissions Reports

### What is a Basic Permissions Report?

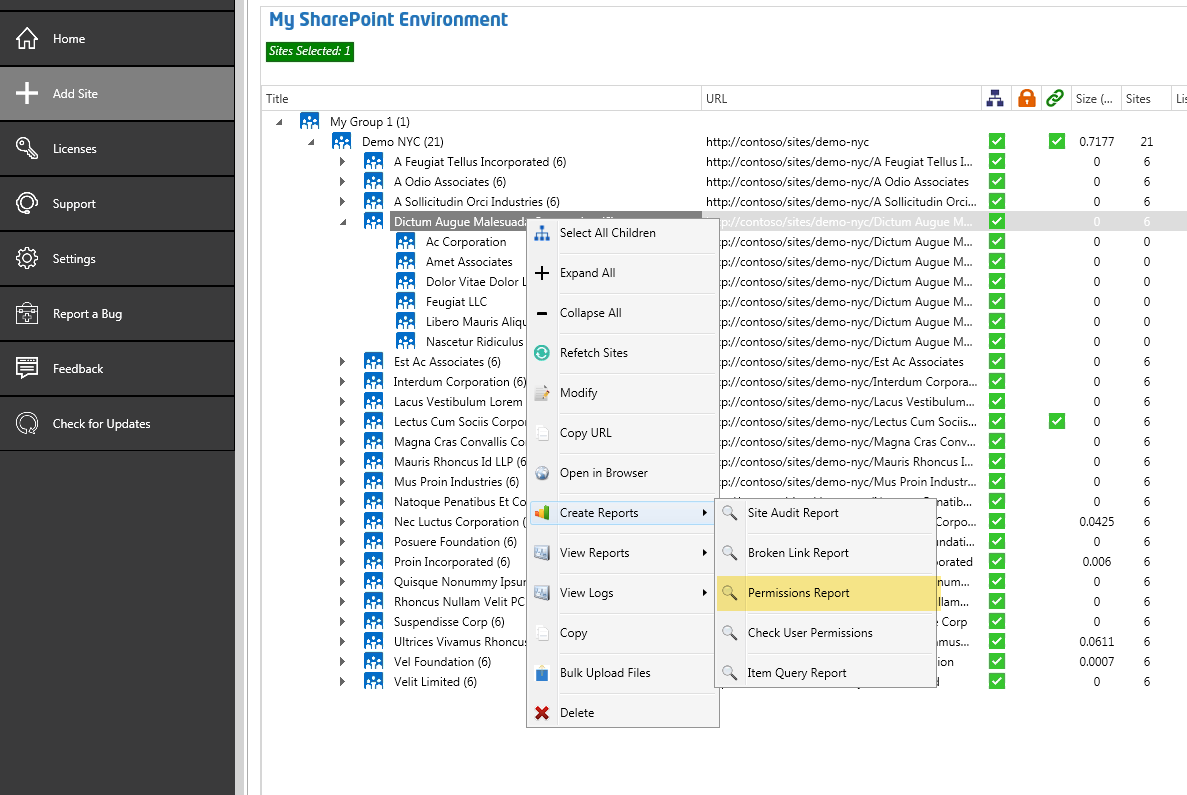
A Basic (Site) Permissions Report will display all permissions for a specific site. The report will contain all of the permissions set at the Site, List and Item level.

### How to Create a Basic Permissions Report

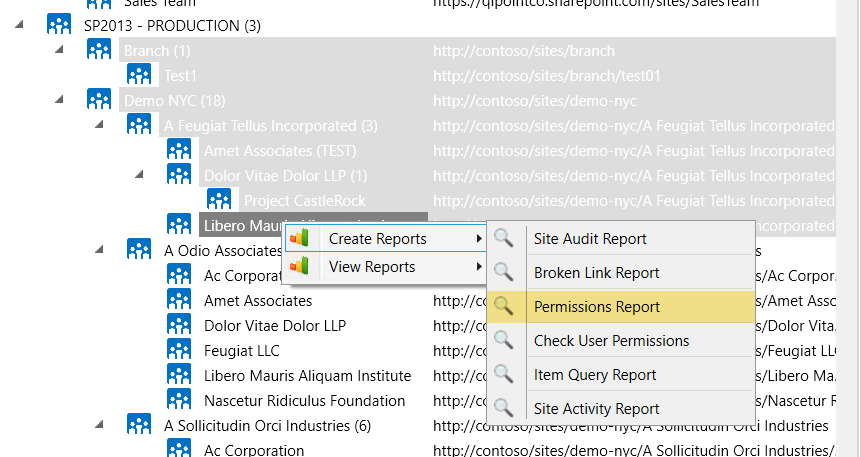


There are 2 ways you can create a Basic Permissions Report.

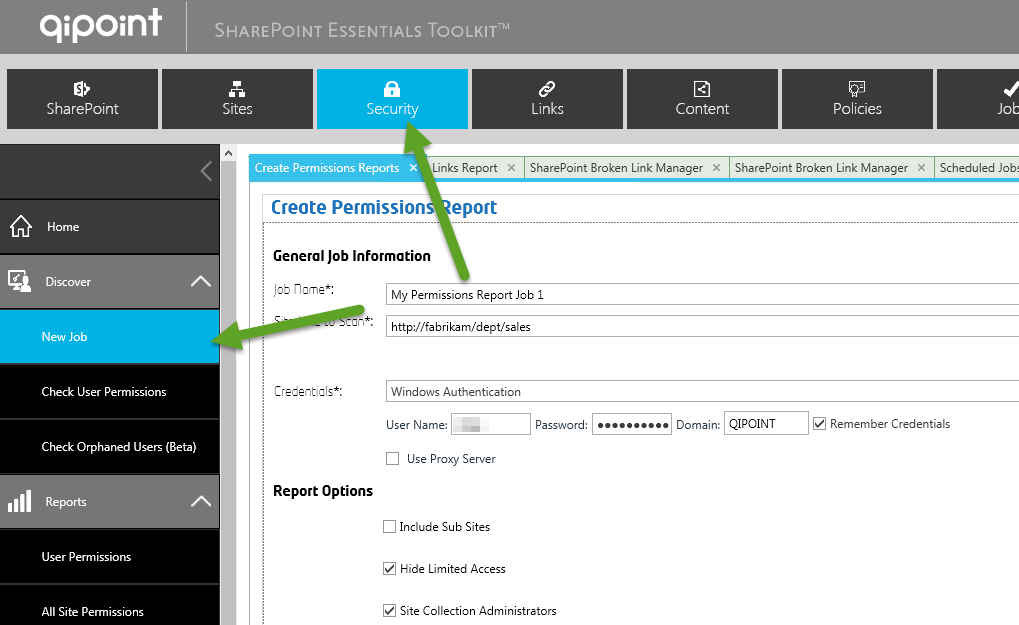
1. From the Home Page Dashboard, right click on a site (that you want to build a report for) and click “Create Reports” -> “Permissions Report”



Alternatively, you can also hold SHIFT or CTRL to multi-select sites to build permission reports for multiple sites



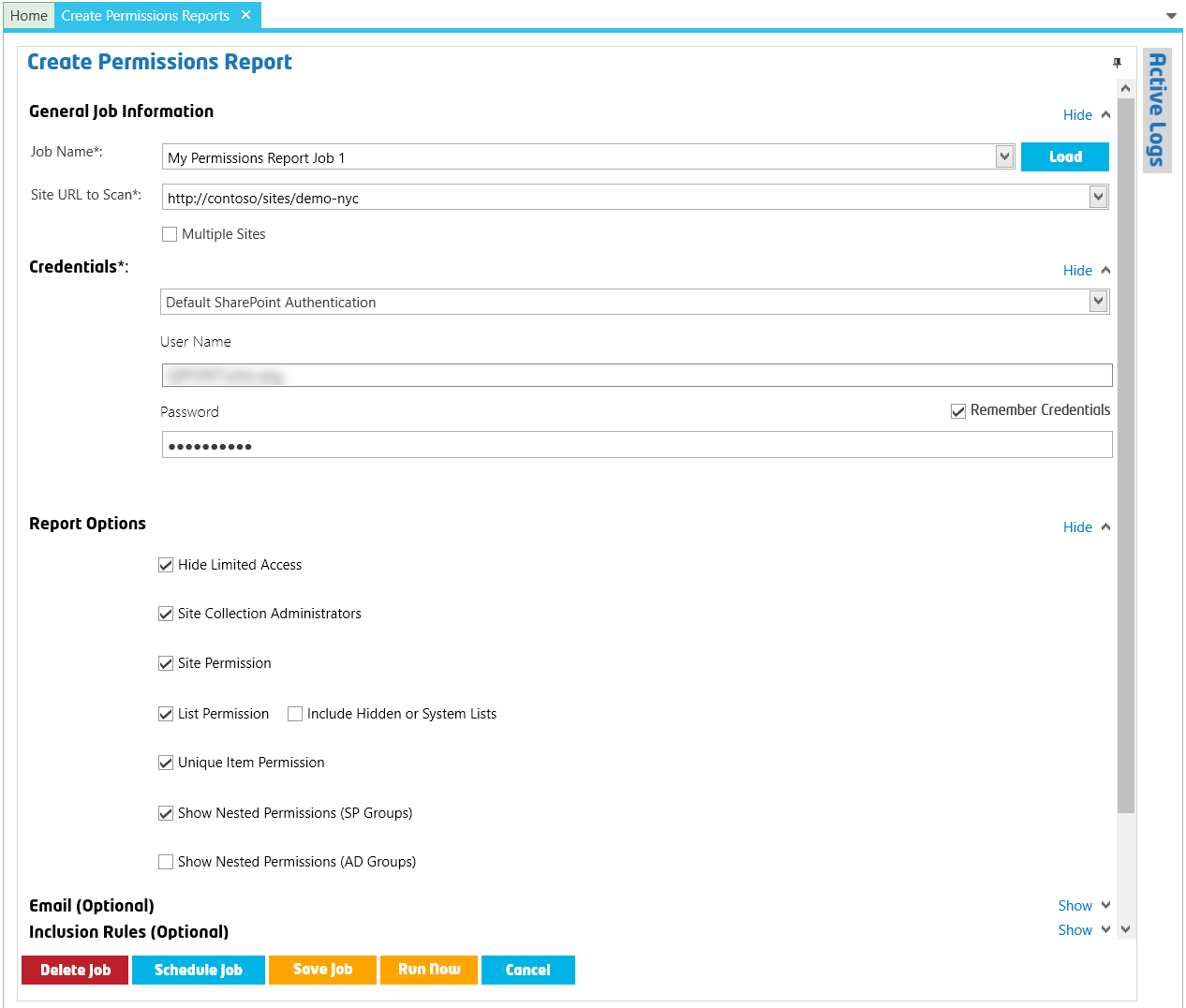
1. Another way to create Basic Permission reports is by clicking on the “Security” button in the Top Navigation, then clicking on the “Discover” button in the Left Navigation to expand it, and then click “New Job”



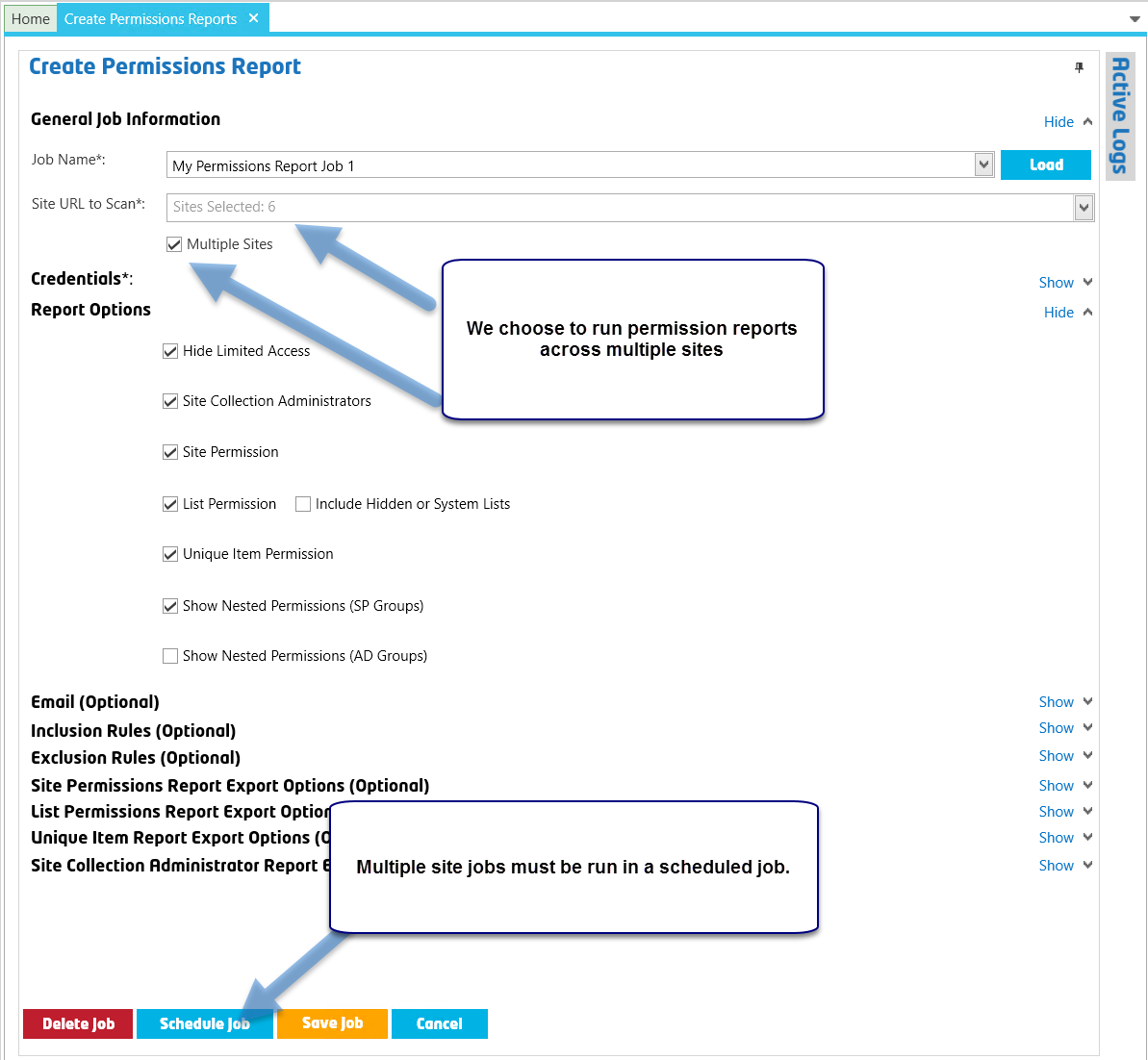
#### Start a Permissions Report Job

1. Open “SharePoint Essentials ToolkitTM”
2. Use one of the options above to open the Permissions Manager “New Job” window
3. A “New Job” window will appear called “Create Permissions Report” (below screenshot)

(NOTE: This page below may appear different depending on the version you are using)



The below is an example if you select multiple sites to run a ‘multi-threaded job’. This allows you to run jobs across multiple sites at the same time.



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

See “Scan Options” (next section) for a description of each option

1. Click “Run Now” button to start the job (or click “Schedule Job”: if this is a job for multiple sites.

#### Scan Options

##### Job Name

This is the Name of the job. A folder will be created in the report directory for every job. The job name will be used as the report name and will be used to help identify the report if scheduled. You must rename the job if you want to save the job for future re-use, or save the job as a template.

##### Site URL to Scan

This is the absolute URL of the site you want to scan to create the permission reports. This can be the path to a Site Collection top level (root) site, or a sub site.

**Example:** <https://companyportal/sites/hr> or <https://companyportal/sites/hr/projects/capital_site/>

Do not include the page path in the URL.

Multiple Sites  
Select this option to run a ‘multi-threaded job’. If this option is selected, you will NOT be able to run a manual job using ‘Run Now’, you need to schedule the job as it will be broken down into one job per site. These jobs will run in parallel and can be viewed from the Scheduled Jobs section. Once complete, job reports can be accessed from the Scheduled Jobs page, the Job History page and also from the Home Page Dashboard by right clicking on one or more of the sites.

##### Credentials

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

**Default SharePoint Authentication** – Automatically determines Authentication to connect to the SharePoint site. This will work in most cases when SharePoint is hosted on your internal company network. Enter the custom credentials to use for this site. If your environment is using a custom login screen, such as one that requires Multi-Factor Authentication/a PIN, is using ADFS, or has SSO enabled, use Web Based Authentication below.

**Office 365** – Use this option to connect to Office 365 hosted SharePoint sites. This applies to both Office 365 non-federated environments. If using a Federated/ADFS enabled Office 365 environment or if your Office 365 environment is using a custom login screen, such as one that requires a PIN, use Web Based Authentication below.

**Web Based Authentication** – Use this option to force the tool to prompt you with a pop up window that will display your company login page to provide credentials. If you are using Office 365 with an ADFS server with custom login page, Multi-Factor Authentication/a PIN, is using ADFS, or has SSO enabled, use this authentication type. If you want to schedule jobs, click to “Remember Credentials” and run the job once, it will remember these credentials for the scheduled job.

**Remember Credentials -** Select this option to store the username and password. Passwords are stored using strong ‘salted’ encryption.

##### Report Options

**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 Collection Administrators** – Select this option to build a report on the Site Collection Administrators for the site.

**NOTE:** A list of all Site Collection Administrators can be generated using the “All Site Collection Administrators” report, which combines all Site Collection Administrator reports found into one.

**Site Permission** – Select this option to build a report on Site-level permissions including users, groups and their respective permission levels. A Site Permissions report will be generated to display the permissions granted at the site-level. This includes both inherited and uniquely given permissions, this can be grouped or filtered in the report after it is created.

**NOTE:** After you generate multiple Site Permission reports, a list of all Site Permissions can be generated using the “All Site Permissions” report, which combines all Site Permission reports found into one. You can also select multiple sites (by holding SHIFT or CTRL and selecting) on the Home Page Dashboard to view a ‘merged report’.

**List Permission** – Select this option to build a report on List permissions including users, groups and their respective permission levels. A List Permissions report will be generated to display the permissions granted at the list-level, for all lists found in the site. This includes both inherited and uniquely given permissions, this can be grouped or filtered in the report after it is created.

**NOTE:** After you generate multiple List Permission reports, a list of all List Permissions can be generated using the “All List Permissions” report, which combines all List Permission reports found into one. You can also select multiple sites (by holding SHIFT or CTRL and selecting) on the Home Page Dashboard to view a ‘merged report’.

**Include System Lists** – Select this option to include hidden system lists in the List & Unique Item Permissions reports.

**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. A Unique Item Permissions report will be generated to display the permissions granted for all uniquely permissioned items for all lists found in the site.

**NOTE:** After you generate multiple Item Level Permission reports, a list of all Item Level Permissions can be generated using the “All Unique Item Permissions” report, which combines all Unique Item Permission reports found into one. You can also select multiple sites (by holding SHIFT or CTRL and selecting) on the Home Page Dashboard to view a ‘merged report’.

**Show Nested Permissions (SP Groups)** – Select this option to display user permissions nested within SharePoint Groups. 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 SharePoint Groups.

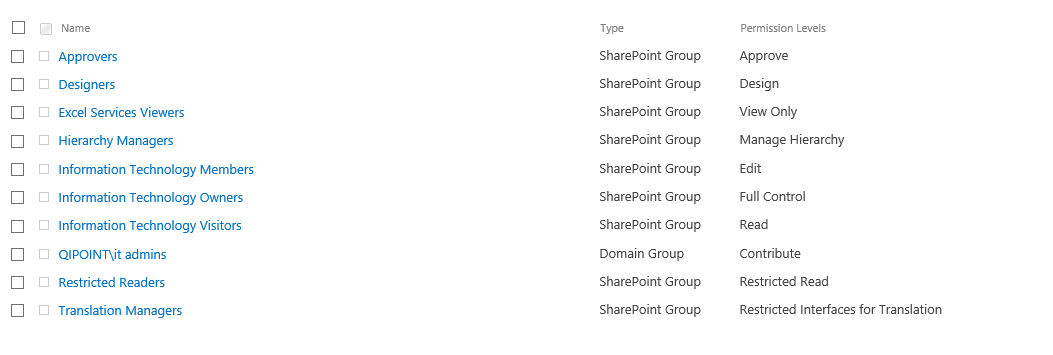
If this option is turned on (checked), the tool will also display all permissions, such as AD Users and AD Groups, nested within all SharePoint Groups found.

The column “Granted Through” will display if the user permissions was granted through a SharePoint Group or was given access Directly.

Example:

Below are permission objects for a site, if ‘Show Nested Permissions (SP Groups)’ is disabled, only these objects below will show in the report. If ‘Show Nested Permissions (SP Groups)’ is enabled, these objects and all AD Users and AD Groups within the SharePoint Groups.

In below example, all users and AD Groups below each group labelled with Type = “SharePoint Group” will be included in the report. Such as “Approvers”, “Designers”, “Excel Services Viewers”, “Hierarchy Managers”, “Information Technology Owners”, “Information Technology Members”, “Information Technology Visitors”, etc…



**Show Nested Permissions (AD Groups)** – (SharePoint on-premise only) Select this option to display user permissions nested within Active Directory (AD) Groups (AD Group memberships). For example:

If this option is turned ON (checked), the tool will also display all permissions, such as AD Users and AD Groups, nested within all AD Groups found.

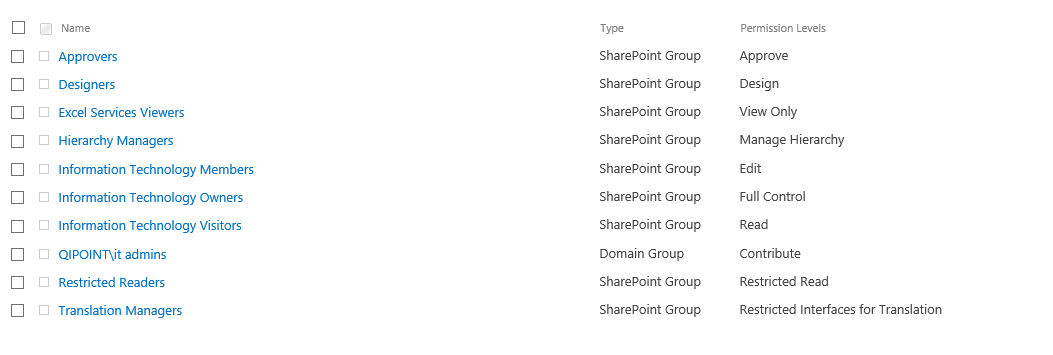
If this option is NOT selected (unchecked), only SharePoint Groups, AD Groups and Users will be displayed in the report that have been given access DIRECTLY in SharePoint, it will not display users or groups nested within the AD Groups.

The column “Granted Through” will display if the user permissions was granted through an AD Group, SharePoint Group or was given access Directly.

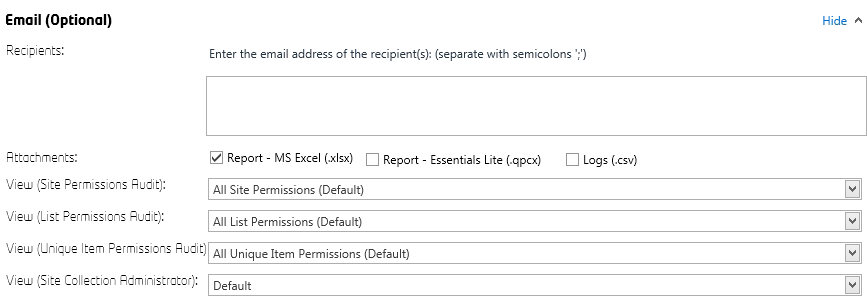
Example:

Below are permission objects for a site, if ‘Show Nested Permissions (AD Groups)’ is disabled, only these objects below will show in the report. If ‘Show Nested Permissions (AD Groups)’ is enabled, these objects and all AD Users and AD Groups within the AD Groups.

In below example, there is one visible AD Group labelled “QIPOINT\it admins” (labelled with Type = “Domain Group”). With the option “Show Nested Permissions (AD Groups)” enabled, all users and group memberships under this “IT Admins” group will also be displayed in the report. NOTE: the tool will also display AD Group memberships for any AD Group found within SharePoint Groups as well.



##### Email



You can optionally enter one or more email addresses for the users who you would like the report to be emailed to. Separate multiple email addresses with a semi-colon ‘;’. Once the report is completed, it will attempt to email the recipients found in this list.

TIP: Enter <Contact Email> for the email address to use the ‘Contact Email’ specified for the site in the Home Page Dashboard. For more information, see the “SharePoint Essentials Toolkit User Manual”.

**Attachments**

*Report - MS Excel (.xlsx)*   
Optionally include the MS Excel report as an attachment. This option is set to Yes (checked) by default. A custom View (see below) can be specified below to set custom filters and groupings to the MS Excel file that is emailed.

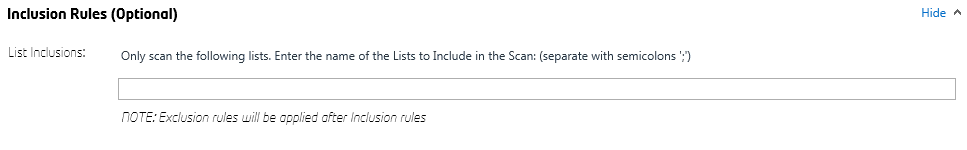
*Report – Essentials Lite (.qpcsv)*   
Optionally include a QiPoint Essentials Lite report as an attachment. The client must have the QiPoint Essentials Lite Client (ClickOnce application) installed on their computer to open this type of report.

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

**View** – (Only applies to MS Excel Report, not SharePoint List Exports or QiPoint Essentials Lite Client reports.) Select the view to use when creating the report. These views can be created from the Permissions Report page (See [Customizing the Report->Views](#_Views) for more information).

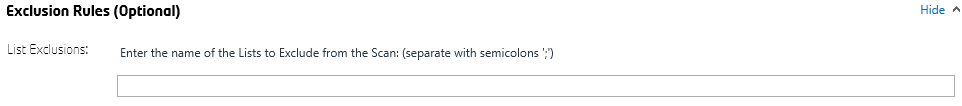
You can select a custom view from the drop-down list to apply it to the MS Excel file that is emailed to user(s). All grouping, sorting and filtering set in these views will be applied to the MS Excel report emailed. If you use the default view, the MS Excel will show a flat list without any grouping or filtering.

##### Inclusion Rules



You can use inclusion rules to only run the job against a specific list. Enter the SharePoint List Display Name/Title (not URL) to only include that list in the report. You can specify multiple lists here, separated by semi-colons.

##### Exclusion Rules



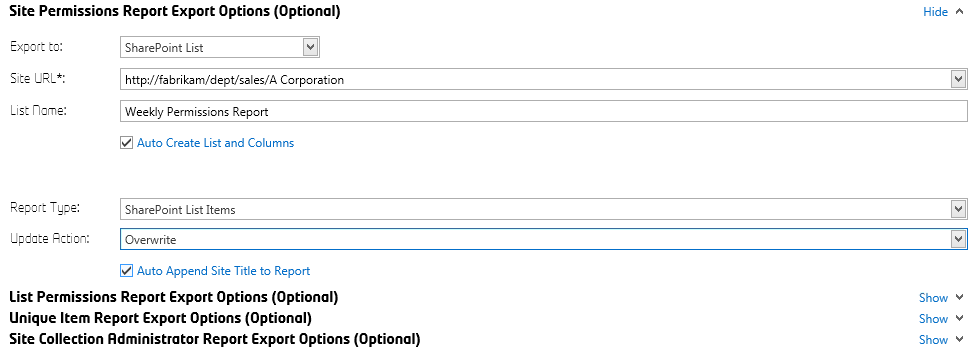
You can use exclusion rules to exclude certain lists in the job. Enter the SharePoint List Display Name/Title (not URL) to exclude that list in the report. You can specify multiple lists here, separated by semi-colons.

##### Export Options



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.

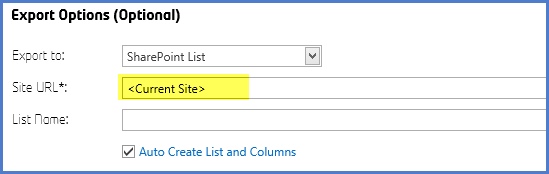
###### Export to SharePoint List



**Site URL**

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

<Current Site> - You can use this token / keyword to use the currently scanned site. If you have performed a ‘multi-threaded’ job by holding SHIFT or CTRL from Home Page Dashboard, this will export the report to the current site being scanned.



**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 ‘Weekly Permissions Report’, and the Site Title is ‘Information Technology’, the SharePoint List report that will be generated will be titled “Weekly Permissions Report - Information Technology”

**Report Type**

You can choose to export the report to a SharePoint List as:

1. SharePoint List Items

NOTE: for reports with many permission objects, such as if you enabled “Show Nested Permissions (AD Groups)” and have 10K+ users in an AD Group, this option may make the list a “Large List” of over 5000 items. If you have many permission objects and do not want to reach this threshold, please use one of the other options below)

1. MS Excel File – The report will be uploaded as a MS Excel File
2. QPCX File (SharePoint Essentials Lite Client format) – The report will be uploaded as a .qpcx file. This file type can be then opened by any end user who installs our free SharePoint Essentials Lite Client (WPF ClickOnce application).



**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 Jobs for Multiple Sites***): 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, and you are exporting to a SharePoint List, 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. If the “Report Type” is set to MS Excel or QPCX formats, this option will append the new report by adding a date time stamp to the file name. You can turn off “Append” and turn on the library versioning to always show the most recent Permissions report and have old versions drop off based on the library major versions limit.

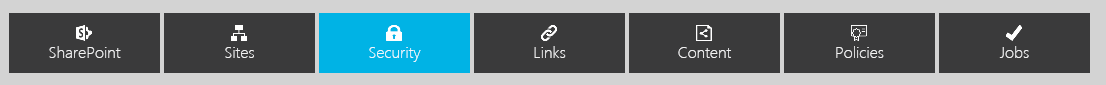
Update: (Available for SharePoint List Item Export) This will refresh the list of entries in the SharePoint Report for this site. If you are using a scheduled job for multiple sites that will add SharePoint List Items to the SAME SharePoint ‘Report’ List, you can use this option so that the report data is always ‘Updated’ for the site being reported on.

## Check User Permissions Reports

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 report will show access granted via SharePoint Group or direct access (where the user was added directly to the site/list/item). You can also optionally “Include AD Group Memberships” to check the user access that has been granted through an AD Group in SharePoint.

This type of report is different than the “Basic (Site) Permissions Report” (above) as this report 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.

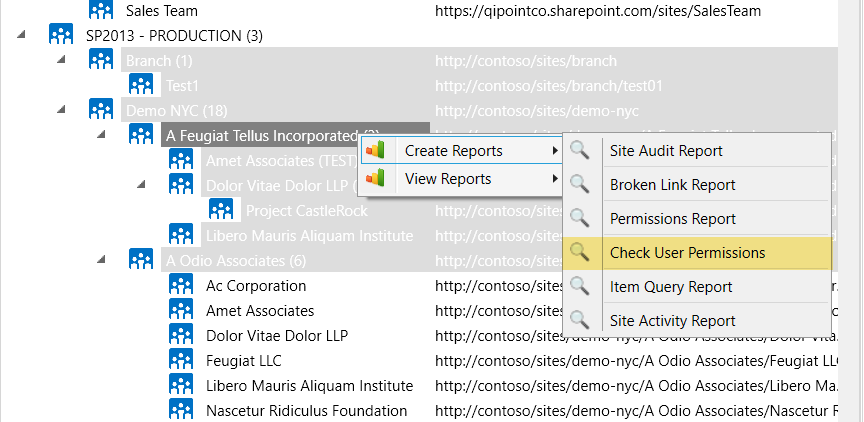
### How to Create a User Permissions Report



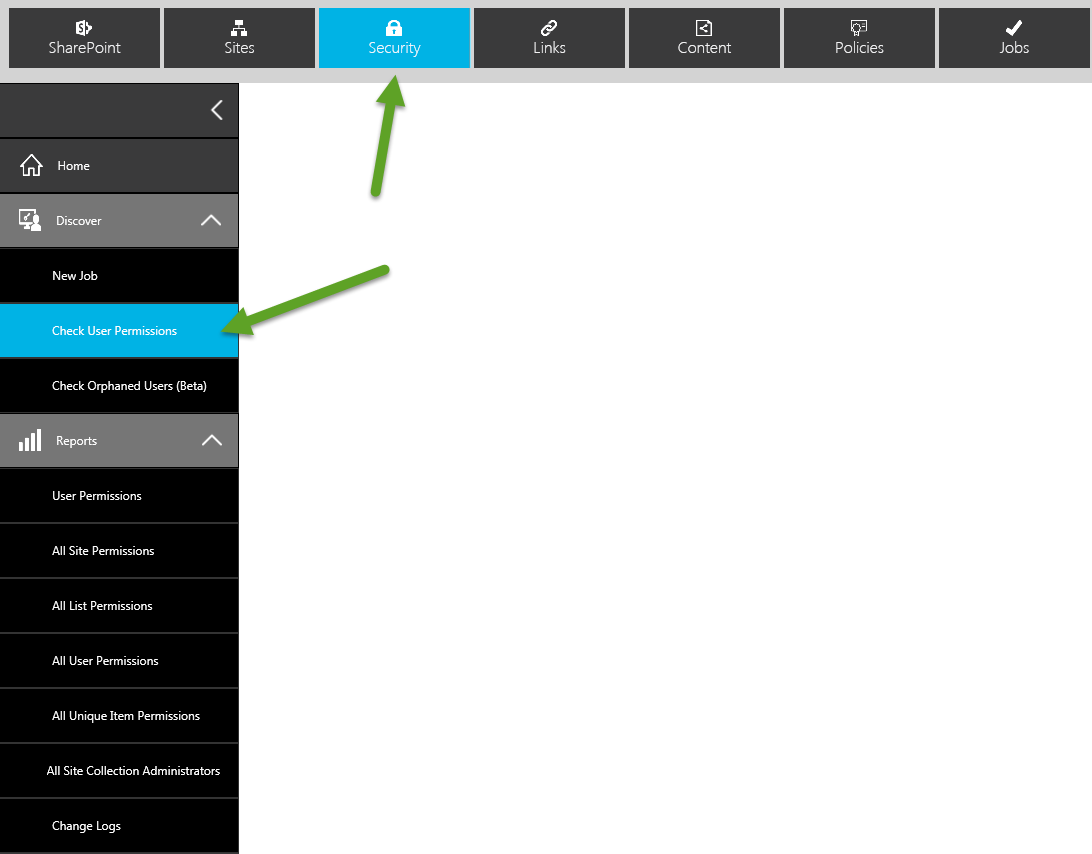
To create this type of report, you have 2 options:

1. From the Home Page Dashboard, select one or more sites (hold SHIFT or CTRL to multi-select sites). Then right click and click ‘Create Reports->Check User Permissions’

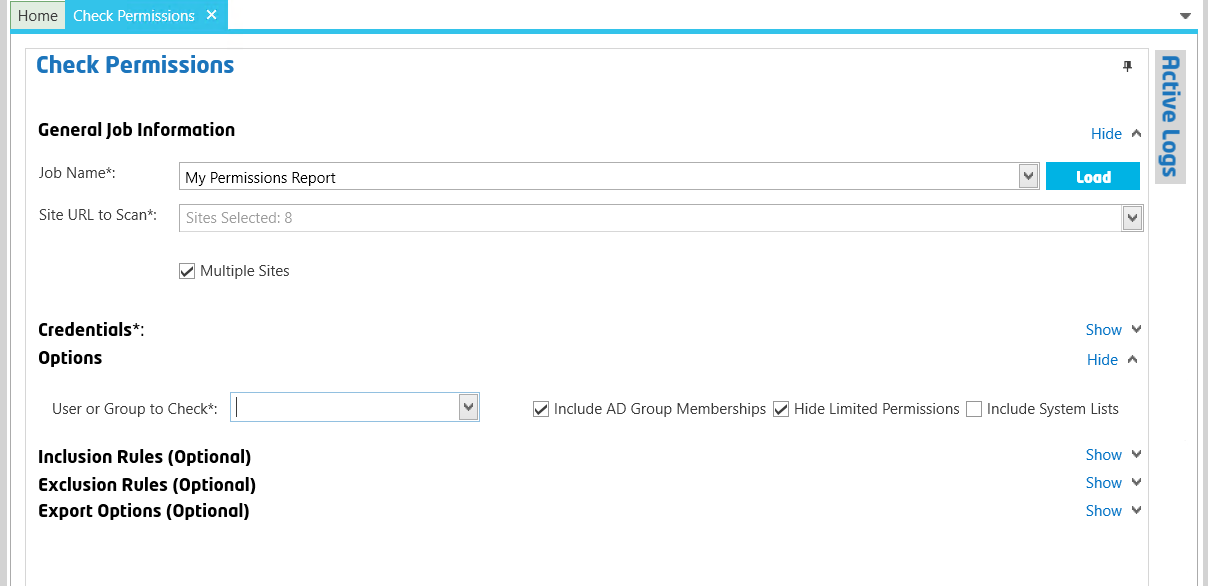
Below I chose to check a user’s permissions across multiple sites in 2 site collections:



1. Alternatively, you can Click on the “Security” button in the Top Navigation, click on the “Discover” button in the Left Navigation to expand it, then click “Check User Permissions”



1. A new “Check Permissions” window will appear (below)



1. From here you can change the Job Name and enter the Site URL for the permissions scope (where you want to check for the user’s permissions).
2. Enter credentials of the account to be used to check the permissions
3. In the Options section, enter the display name/email or account name of the user/group who you want to check permissions for. The tool will try to give you some suggestions based on your input here. You may see multiple display names if multiple accounts are found for that user.
4. Click “Run Now” button to create the report. If multiple sites are selected, it will iterate all sites and build a single report.

#### Check Permissions Fields

##### Job Name

This is the Name of the job. A folder will be created in the report directory for every job. The job name will be used as the report name and will be used to help identify the report if scheduled. You must rename the job if you want to save the job for future re-use, or save the job as a template.

##### Credentials

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

**Default SharePoint Authentication** – Automatically determines Authentication to connect to the SharePoint site. This will work in most cases when SharePoint is hosted on your internal company network. Enter the custom credentials to use for this site. If your environment is using a custom login screen, such as one that requires Multi-Factor Authentication/a PIN, is using ADFS, or has SSO enabled, use Web Based Authentication below.

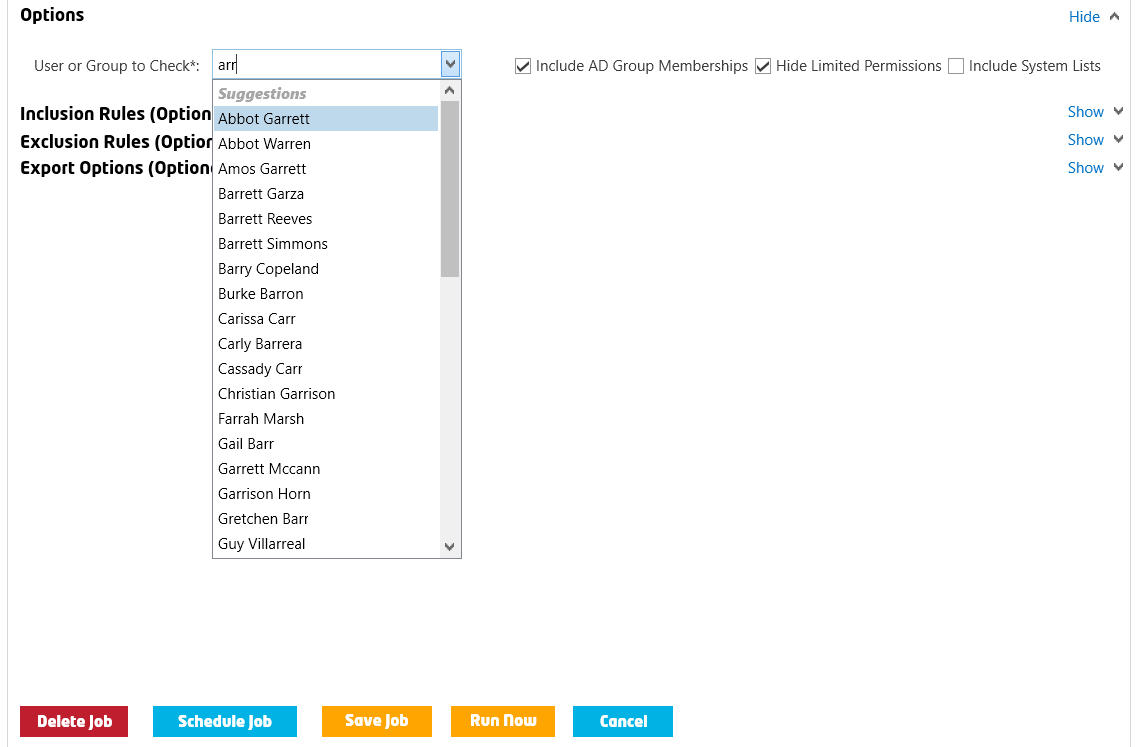
**Office 365** – Use this option to connect to Office 365 hosted SharePoint sites. This applies to both Office 365 non-federated environments. If using a Federated/ADFS enabled Office 365 environment or if your Office 365 environment is using a custom login screen, such as one that requires a PIN, use Web Based Authentication below.

**Web Based Authentication** – Use this option to force the tool to prompt you with a pop up window that will display your company login page to provide credentials. If you are using Office 365 with an ADFS server with custom login page, Multi-Factor Authentication/a PIN, is using ADFS, or has SSO enabled, use this authentication type. If you want to schedule jobs, click to “Remember Credentials” and run the job once, it will remember these credentials for the scheduled job.

**Remember Credentials -** Select this option to store the username and password. Passwords are stored using strong ‘salted’ encryption.

##### Options

**User or Group to Check** – Enter the AD User, AD Group or SharePoint Group account name to check. The tool will attempt to provide suggestions for the user based on LDAP queries to your Directory Server.

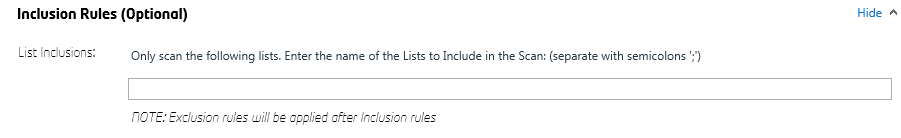


**Include AD Group Memberships** – Select this option to check membership within AD Groups for the specified account. This applies to AD User or AD Group accounts in the “User or Group to Check”, this does not apply to SharePoint Groups entered in the “User or Group to Check” textbox.

**Hide Limited Permissions** – 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>

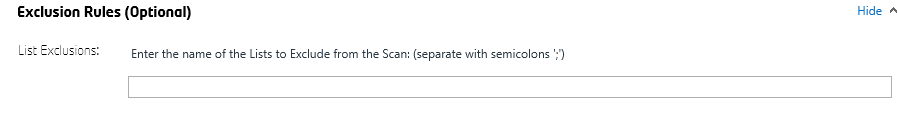
**Include System Lists** – Scans all permissions within Hidden System lists and libraries.

### Inclusion Rules (Optional)



**List Inclusions** - Use this section to filter and only scan specific SharePoint Lists in the job. Use List Title (display name), not the List URL here. The user can specify what Lists to include in the report by entering the names lists in this section. If the name of the list exists in multiple sites, they will all be included if the List title (display name) matches. Wildcards (\*) are supported, so if you want to include all lists and libraries that have the word ‘documents’ in the List Title, you can enter “\*documents\*” and all lists and libraries with ‘documents’ will be included in the scan. These values are not case-sensitive. Once a match is found, all permissions within the list and its items will be scanned (inclusion rules do not apply to page/item/file contents). Separate Lists using semi-colons ‘;’.

### Exclusion Rules (Optional)

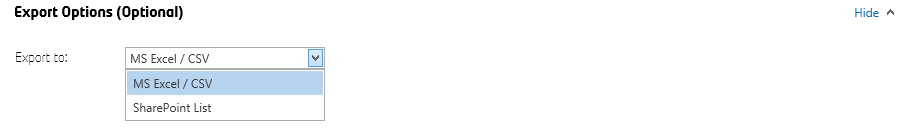


**List Inclusions** - Use this section to filter and only scan specific SharePoint Lists in the job. Use List Title (display name), not the List URL here. The user can specify what Lists to include in the report by entering the names lists in this section. If the name of the list exists in multiple sites, they will all be included if the List title (display name) matches. Wildcards (\*) are supported, so if you want to

### NOTE: Inclusion/Exclusion Rules:

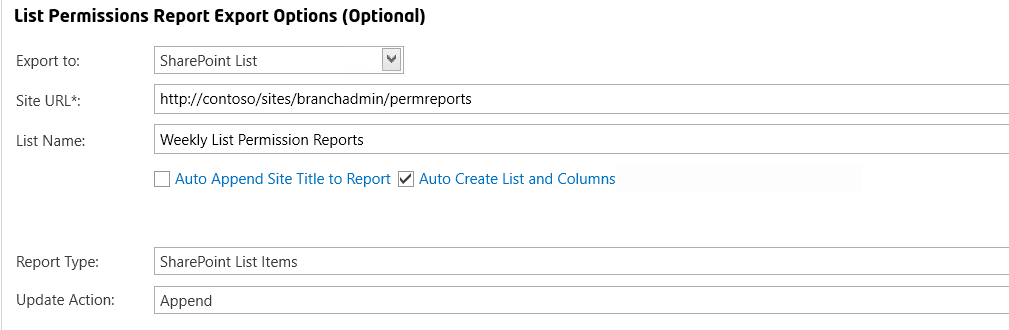
* **Exclusion rules are applied AFTER Inclusion rules (if any).**

### Export Options



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.

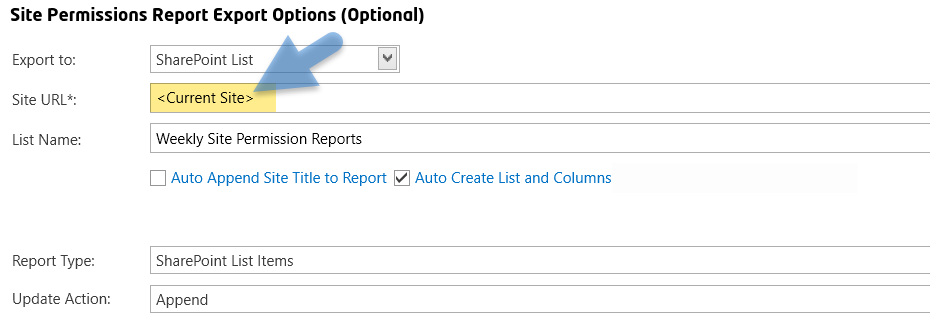
#### Export to SharePoint List



**Site URL**

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

<Current Site> - You can use this token / keyword to use the currently scanned site. If you have performed a ‘multi-threaded’ job by holding SHIFT or CTRL from Home Page Dashboard, this will export the report to the current site being scanned.



**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 ‘Weekly User Permissions Report’, and the Site Title is ‘Information Technology’, the SharePoint List report that will be generated will be titled “Weekly User Permissions Report - Information Technology”

**Report Type**

You can choose to export the report to a SharePoint List as:

1. SharePoint List Items

NOTE: for reports with many security objects (such as if you enable “Include AD Group Memberships” and have over 5000 account memberships within one or more AD Groups), this option may make the list a “Large List” of over 5000 items. If you have many permission objects and do not want to reach this threshold, please use one of the other options below)

1. MS Excel File – The report will be uploaded as a MS Excel File
2. QPCX File (SharePoint Essentials Lite Client format) – The report will be uploaded as a .qpcx file. This file type can be then opened by any end user who installs our free SharePoint Essentials Lite Client (WPF ClickOnce application).



**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 Jobs for Multiple Sites***): 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, and you are exporting to a SharePoint List, all sites being scanned in the job will be merged into one single report (a single SharePoint List).

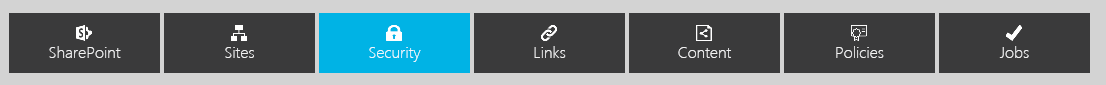
**Update Action**

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. If the “Report Type” is set to MS Excel or QPCX formats, this option will append the new report by adding a date time stamp to the file name. You can turn off “Append” and turn on the library versioning to always show the most recent Permissions report and have old versions drop off based on the library major versions limit.

Update: (Available for SharePoint List Item Export) This will refresh the list of entries in the SharePoint Report for this site. If you are using a scheduled job for multiple sites that will add SharePoint List Items to the SAME SharePoint ‘Report’ List, you can use this option so that the report data is always ‘Updated’ for the site being reported on.

## Check Orphaned Users



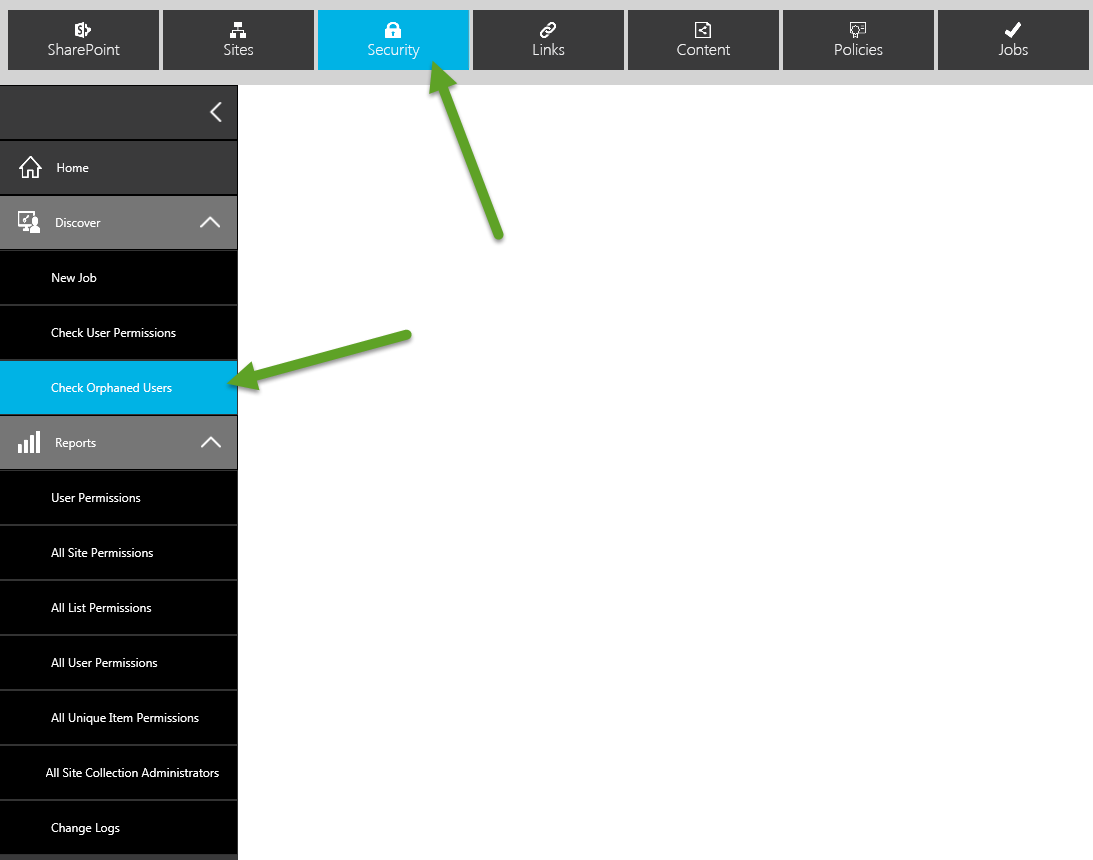
This creates a report that shows all orphaned users. An “Orphaned User” is a user object in SharePoint that does not have a corresponding Active Directory (AD) Account. This could be a disabled or deleted AD user or group account.

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

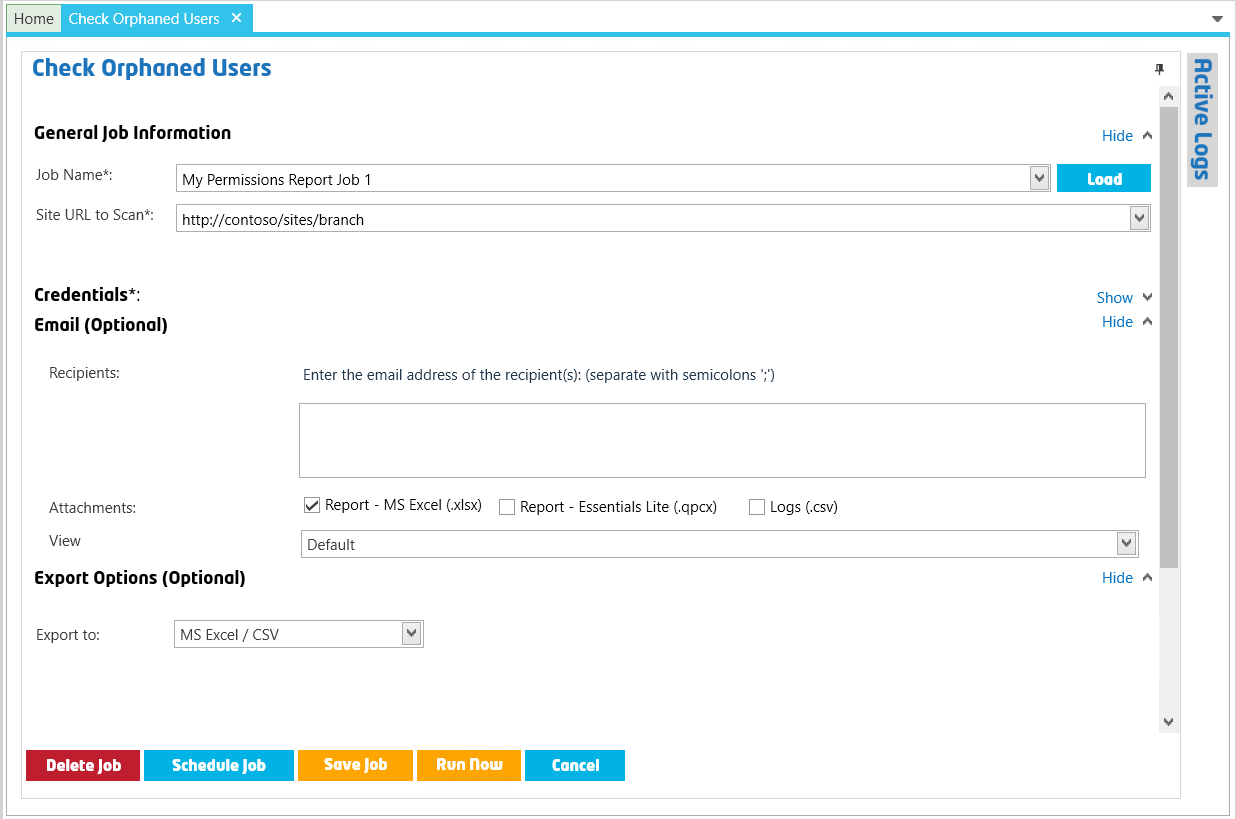
### How to Create an Orphaned Users Report

To create this type of report,

1. Click on the “Security” button in the Top Navigation, click on the “Discover” button in the Left Navigation to expand it, then click “Check Orphaned Users”



1. A new “Check Orphaned Users” window will appear (below)



1. You can enter a Job Name or leave the default.
2. Enter or select the Site to check in ‘Site URL to Scan’
3. Enter any other options here, more info on these fields below.
4. Click “Run Now” button to create the report.

#### Scan Options

##### Job Name

This is the Name of the job. A folder will be created in the report directory for every job. The job name will be used as the report name and will be used to help identify the report if scheduled. You must rename the job if you want to save the job for future re-use, or save the job as a template.

##### Site URL to Scan

This is the absolute URL of the site you want to scan to create the permission reports. This can be the path to a Site Collection top level (root) site, or a sub site.

**Example:** <https://companyportal/sites/hr> or <https://companyportal/sites/hr/projects/capital_site/>

Do not include the page path in the URL.

##### Credentials

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

**Windows Authentication** – Uses Windows Authentication to connect to the SharePoint site. This will work in most cases when SharePoint is hosted on your internal company network. Enter the custom credentials to use for this site. If your environment is using a custom login screen, such as one that requires a PIN, is using ADFS, or has SSO enabled, use Web Based Authentication below.

**Claims Based Authentication** – Connects to the SharePoint site using Claims Based authentication. This is the default authentication method for SharePoint 2013. If you are using Azure to host SharePoint, you can use this authentication method.

**Office 365** – Use this option to connect to Office 365 hosted SharePoint sites. This applies to both Office 365 non-federated environments. If using a Federated/ADFS enabled Office 365 environment or if your Office 365 environment is using a custom login screen, such as one that requires a PIN, use Web Based Authentication below.

Forms Based Authentication – Use this method if the SharePoint site you are connecting to uses Forms based authentication.

**Web Based Authentication** – Use this option to force the tool to prompt you with a pop up window that will display your company login page to provide credentials. If you are using Office 365 with an ADFS server with custom login page, you can use this authentication type. If you want to schedule jobs, click to “Remember Credentials” and run the job once, it will remember these credentials for the scheduled job.

**Remember Credentials -** Select this option to store the username and password. Passwords are stored using strong ‘salted’ encryption.

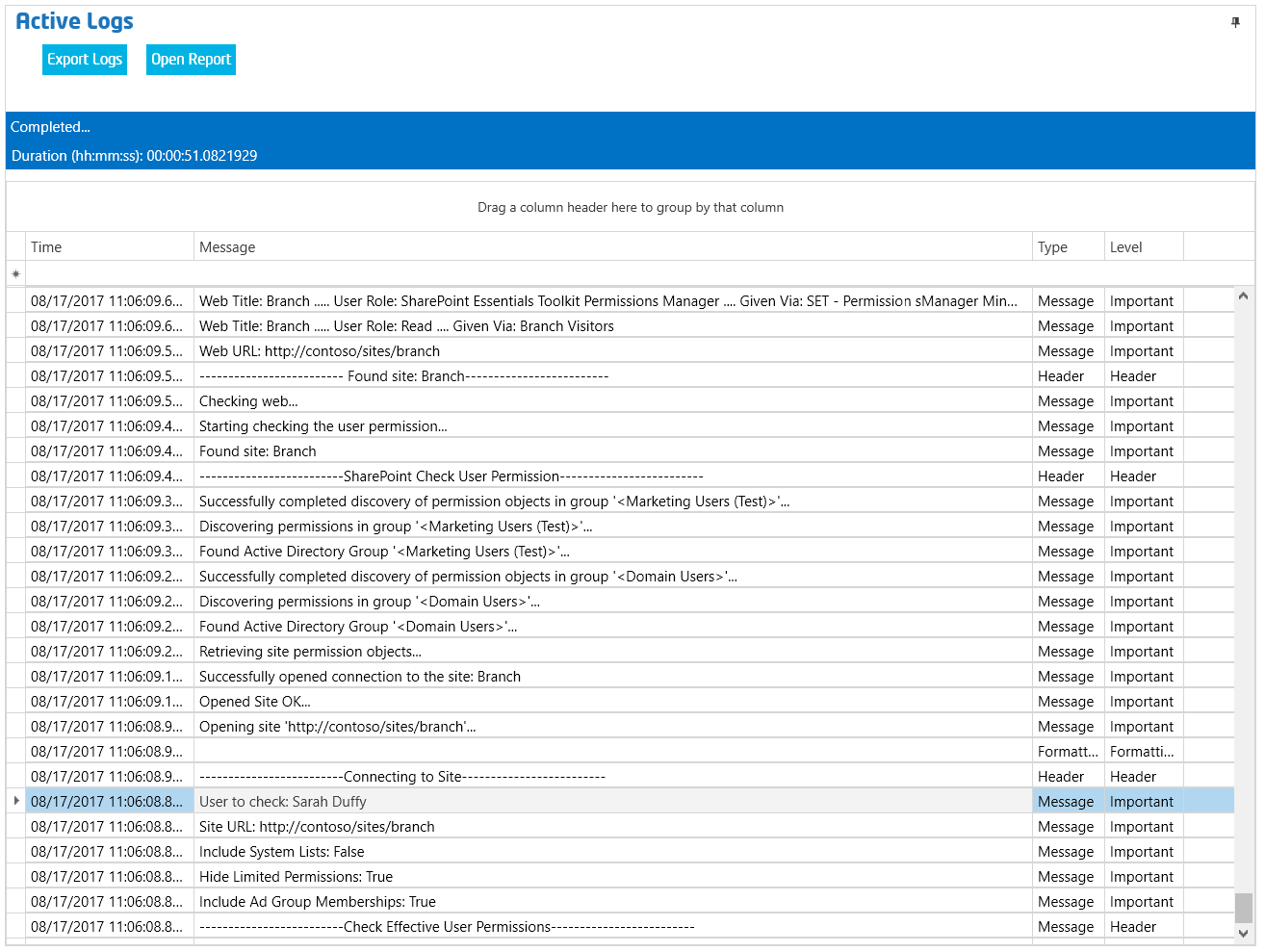
# Logs

As the Job is running, logs will be generated in real-time so that you can view the status and progress.

Log files and reports are stored under the path located in the Settings page (Home -> Settings -> Path to Store Reports).

Normally you can view any log by navigating to the Home Page Dashboard, and right clicking the site you ran the job, and then clicking “View Logs”. You can also view logs from the “Job->Job History” page, or if the job was scheduled, the logs are also accessible from the “Jobs->Scheduled Jobs” window.

Below is an example of the Active Logs page when a job is run manually (not in a schedule). A similar log window will appear when viewing jobs from the “Job History” window or the “Scheduled Jobs” pages.



You can export job logs to CSV format by clicking the Export Logs button.

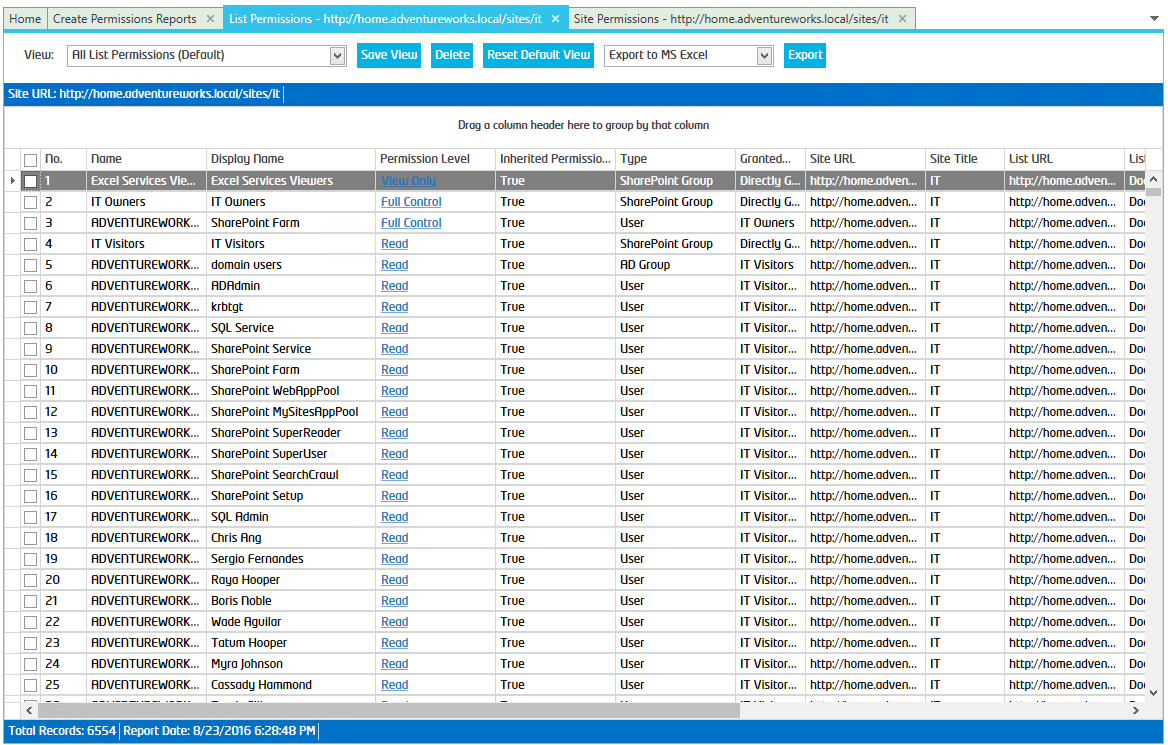


# How to Interpret the Reports

## Interpreting the Reports

The report has a lot of information, you would benefit the best from the reports by dragging and dropping columns to group, and then you can sort, and apply advanced or simple filtering to help to generate a report most useful to your requirements.

For example, group by ‘Display Name’ to view all permissions for a specific user or group account, group by Site URL to further view permissions for users in multiple sites. Use search (CTRL+F) and sort to find something specific. A single permissions report can be across multiple lists, sites, site collections, web applications and even across farms.



### Opening the Report

#### Basic Permissions Report (Site)

There are 4 types of Basic Permissions Reports:

1. Site Permissions Report
2. List Permissions Report
3. Unique Item Permissions Report
4. Site Collection Administrators Report

These are shown below.

Once a scan is complete you can open a Basic Permissions Report in several ways:

* + When a scan is complete, you will have a button on the top right (above the “Active Log”) that says “Open Report”
  + Once you Click “Open Report” and the report opens, you can click “Export” to view the report in SharePoint/CSV/PDF/Excel/QPCX format
  + From the Home Page Dashboard, you can right click on a site that you wish to preview, and click “View Reports -> Permissions Report”
  + From the “Job->Job History” page you can find previously run Jobs and their reports and logs.
  + For scheduled jobs, you can also find the reports and logs under the “Job->Scheduled Jobs” page.
  + To view all report files (CSV and QPCX formats available)
    - Open Windows Explorer and navigate to the path where the reports are stored, the default location is in the user’s My Documents folder under “QiPoint\Reports”. You can change the report path under “Home -> Settings -> Path to Store Reports”

#### Site Permissions - Report Fields

##### No.

Line number. This is used as a reference to help identify items that need to be responded to as they are reviewed. This is not related to the actual permission object and is for reference purposes only.

##### Group

This is the group name that was given to the site during the scan. This does not affect SharePoint data; it is only used for reporting purposes. For example, you can set the name of sites to “Production” or “Test” for different environments.

##### Name

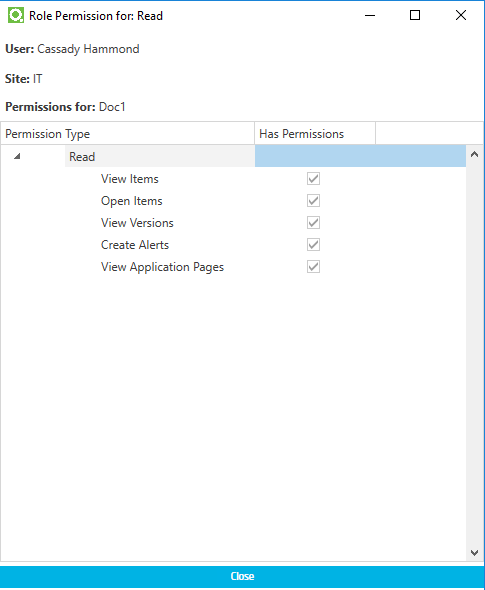
This is the account name. If this is an AD Account, this will be the Logon Name for users or the Group Name for AD Security Groups. If this is a SharePoint Group, it will be the Name of the SharePoint Group.

##### Display Name

This is the account display name. If this is an AD Account, this will be the Display Name. If this is a SharePoint Group, it will be the Name of the SharePoint Group (which will be the same as Name column above).

##### Permission Level

This is the SharePoint Permission Level that the account has. You can click on the Permission Level link and it will open the specific permission roles (for the Permission Level).



##### Permission Level

This is the SharePoint Permission Level that the account has. You can click on the Permission Level link and it will open the specific permission roles (for the Permission Level).

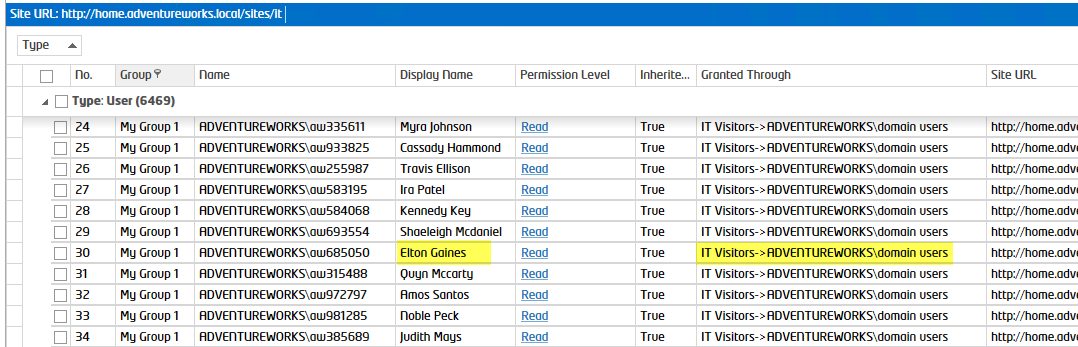
##### Inherited Permissions

This column will specify if the permission for this record was granted directly or if it was permission that was inherited from its parent, such as a SharePoint Subsite that inherits permission from the Root Site Level permissions. “True” = Inherited from parent, “False” = Uniquely defined permissions which were granted directly to this site.

##### Granted Through

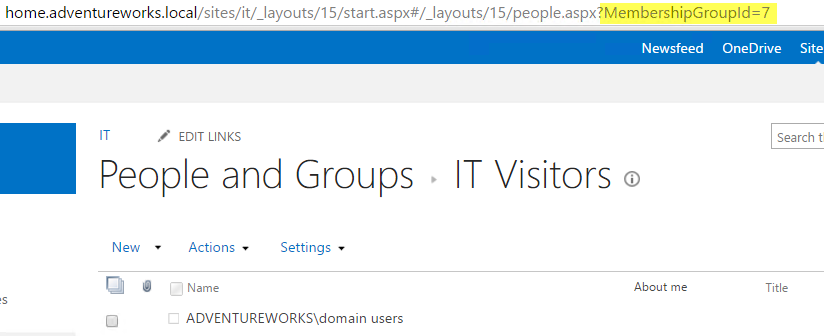
This column will specify how the account (found under column “Name”) was granted access. “Directly Given” = The account was granted access directly to this site, list or item. If this column value is not “Directly Given”, then this account was granted access through a SharePoint Group, an AD Group, or both. The name and path of the group(s) that provided this access will be shown.

Below is an example of an account “Elton Gaines” who was Granted Access Through a SharePoint Group called “IT Visitors” and the AD Group “Domain Users”:



##### Permission ID

This is the SharePoint User ID (SPUserID or MemberShipGroupID). If the account was granted directly, this will show the actual account ID, if the account was Granted Access Through a SharePoint or AD Group, this will display the ID for that “Group” object where the permission was granted through. This can be useful when tracking multiple objects, such as instances of an AD Group that is set in different places.



##### Site URL

This is the URL path to the SharePoint Site that the permission was found.

##### Site Title

This is the Title of the SharePoint Site that the permission was found.

##### Web Id

This is GUID identifier for the site being reported on.

##### SP Version

This is the SharePoint version of the site in the report.

#### List Permissions - Report Fields

##### No.

Line number. This is used as a reference to help identify items that need to be responded to as they are reviewed. This is not related to the actual permission object and is for reference purposes only.

##### Group

This is the group name that was given to the site during the scan. This does not affect SharePoint data; it is only used for reporting purposes. For example, you can set the name of sites to “Production” or “Test” for different environments.

##### Name

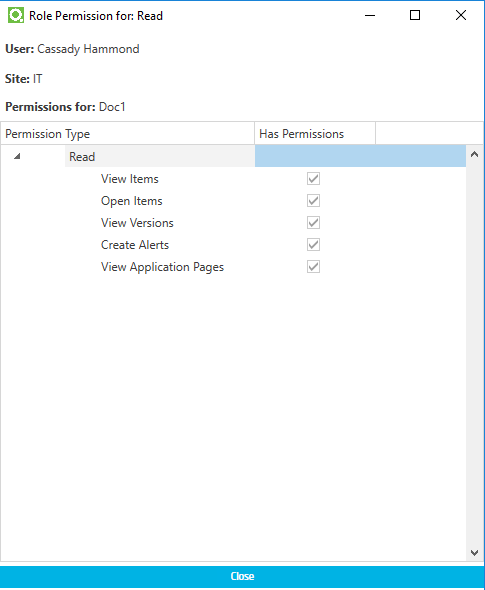
This is the account name. If this is an AD Account, this will be the Logon Name for users or the Group Name for AD Security Groups. If this is a SharePoint Group, it will be the Name of the SharePoint Group.

##### Display Name

This is the account display name. If this is an AD Account, this will be the Display Name. If this is a SharePoint Group, it will be the Name of the SharePoint Group (which will be the same as Name column above).

##### Permission Level

This is the SharePoint Permission Level that the account has. You can click on the Permission Level link and it will open the specific permission roles (for the Permission Level).



##### Permission Level

This is the SharePoint Permission Level that the account has. You can click on the Permission Level link and it will open the specific permission roles (for the Permission Level).

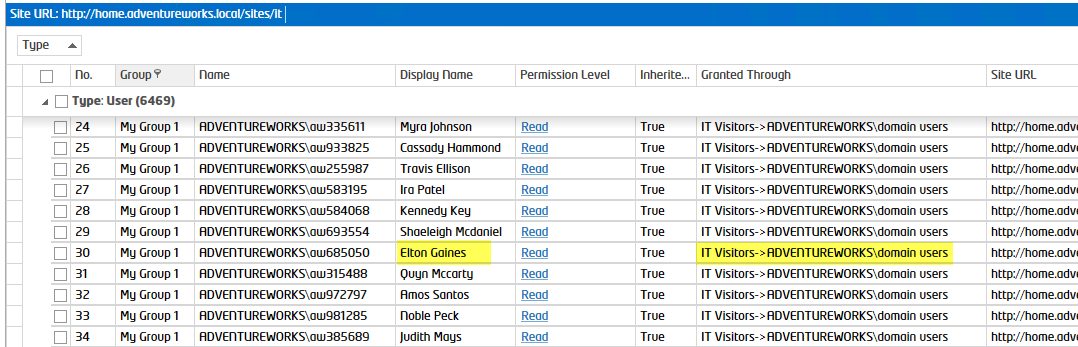
##### Inherited Permissions

This column will specify if the permission for this record was granted directly or if it was permission that was inherited from its parent, such as a SharePoint List that inherits permission from the Site Level permissions. “True” = Inherited from parent, “False” = Uniquely defined permissions which were granted directly to this list.

##### Granted Through

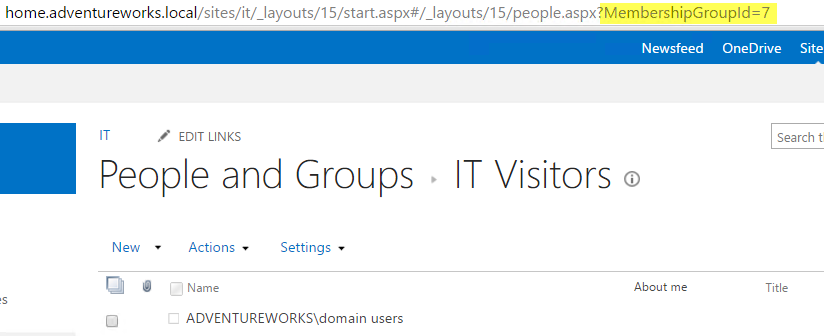
This column will specify how the account (found under column “Name”) was granted access. “Directly Given” = The account was granted access directly to this site, list or item. If this column value is not “Directly Given”, then this account was granted access through a SharePoint Group, an AD Group, or both. The name and path of the group(s) that provided this access will be shown.

Below is an example of an account “Elton Gaines” who was Granted Access Through a SharePoint Group called “IT Visitors” and the AD Group “Domain Users”:



##### Permission ID

This is the SharePoint User ID (SPUserID or MemberShipGroupID). If the account was granted directly, this will show the actual account ID, if the account was Granted Access Through a SharePoint or AD Group, this will display the ID for that “Group” object where the permission was granted through. This can be useful when tracking multiple objects, such as instances of an AD Group that is set in different places.



##### Site URL

This is the URL path to the SharePoint Site that the permission was found.

##### Site Title

This is the Title of the SharePoint Site that the permission was found.

##### List Title

This is the Title of the SharePoint List that the permission was found.

##### List URL

This is the URL of the SharePoint List that the permission was found.

##### Visible

This shows if the SharePoint List is visible or a hidden list.

##### List ID

This is the ID of the SharePoint List that the permission was found.

##### Template ID

This is the Template ID of the SharePoint List that the permission was found.

##### Template Name

This is the Template Name of the SharePoint List that the permission was found.

##### SP Version

This is the SharePoint version of the site in the report.

#### Unique Item Permissions - Report Fields

##### No.

Line number. This is used as a reference to help identify items that need to be responded to as they are reviewed. This is not related to the actual permission object and is for reference purposes only.

##### Group

This is the group name that was given to the site during the scan. This does not affect SharePoint data; it is only used for reporting purposes. For example, you can set the name of sites to “Production” or “Test” for different environments.

##### Name

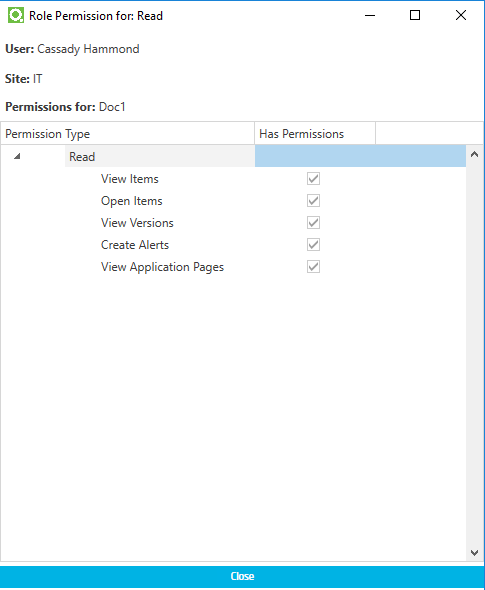
This is the account name. If this is an AD Account, this will be the Logon Name for users or the Group Name for AD Security Groups. If this is a SharePoint Group, it will be the Name of the SharePoint Group.

##### Display Name

This is the account display name. If this is an AD Account, this will be the Display Name. If this is a SharePoint Group, it will be the Name of the SharePoint Group (which will be the same as Name column above).

##### Permission Level

This is the SharePoint Permission Level that the account has. You can click on the Permission Level link and it will open the specific permission roles (for the Permission Level).



##### Permission Level

This is the SharePoint Permission Level that the account has. You can click on the Permission Level link and it will open the specific permission roles (for the Permission Level).

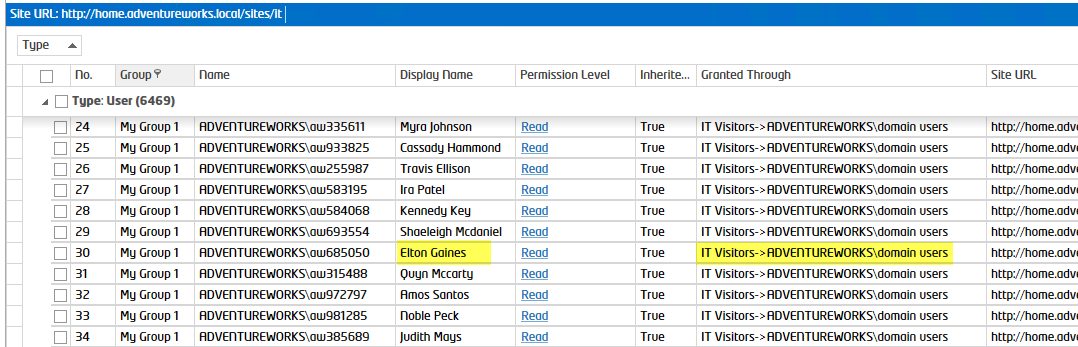
##### Inherited Permissions

This column will specify if the permission for this record was granted directly or if it was permission that was inherited from its parent. This report (Unique Item Permissions will always show False (uniquely given permissions) for items). “True” = Inherited from parent, “False” = Uniquely defined permissions which were granted directly to this item.

##### Granted Through

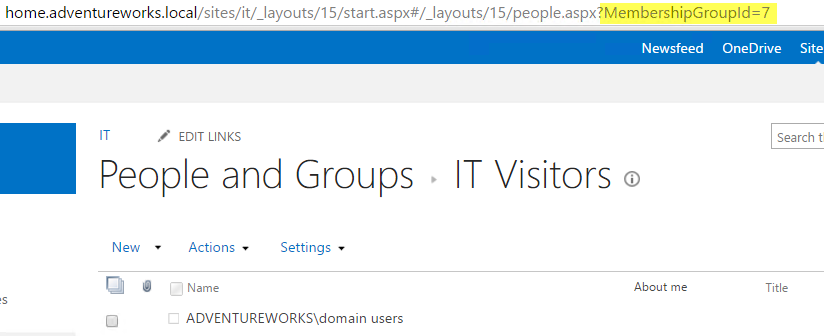
This column will specify how the account (found under column “Name”) was granted access. “Directly Given” = The account was granted access directly to this site, list or item. If this column value is not “Directly Given”, then this account was granted access through a SharePoint Group, an AD Group, or both. The name and path of the group(s) that provided this access will be shown.

Below is an example of an account “Elton Gaines” who was Granted Access Through a SharePoint Group called “IT Visitors” and the AD Group “Domain Users”:



##### Permission ID

This is the SharePoint User ID (SPUserID or MemberShipGroupID). If the account was granted directly, this will show the actual account ID, if the account was Granted Access Through a SharePoint or AD Group, this will display the ID for that “Group” object where the permission was granted through. This can be useful when tracking multiple objects, such as instances of an AD Group that is set in different places.



##### Access Type

This can be either a Folder or Item. This identifies what type of object (folder or file/item) was being reported on.

##### Site URL

This is the URL path to the SharePoint Site that the permission was found.

##### Site Title

This is the Title of the SharePoint Site that the permission was found.

##### List Title

This is the Title of the SharePoint List that the permission was found.

##### List URL

This is the URL of the SharePoint List that the permission was found.

##### Visible

This shows if the SharePoint List is visible or a hidden list.

##### List ID

This is the ID of the SharePoint List that the permission was found.

##### Item Title

This is the Title of the SharePoint List Item that the permission was found.

##### File Name

This is the Name of the SharePoint List Item that the permission was found.

##### Item URL

This is the URL of the SharePoint List Item that the permission was found.

##### Item ID

This is the ID of the SharePoint List Item that the permission was found.

##### SP Version

This is the SharePoint version of the site in the report.

#### Site Collection Administrators - Report Fields

##### No.

Line number. This is used as a reference to help identify items that need to be responded to as they are reviewed. This is not related to the actual permission object and is for reference purposes only.

##### Group

This is the group name that was given to the site during the scan. This does not affect SharePoint data; it is only used for reporting purposes. For example, you can set the name of sites to “Production” or “Test” for different environments.

##### Type

This will identify if the account is either the Primary or Secondary Site Collection Administrator.

##### Name

This is the account name. If this is an AD Account, this will be the Logon Name for users or the Group Name for AD Security Groups. If this is a SharePoint Group, it will be the Name of the SharePoint Group.

##### Display Name

This is the account display name. If this is an AD Account, this will be the Display Name. If this is a SharePoint Group, it will be the Name of the SharePoint Group (which will be the same as Name column above).

##### Site Collection

This is the site collection title.

##### Site Collection URL

This is the site collection URL.

##### Office

The toolkit will attempt to retrieve the contact Office information and display it here.

##### Phone

The toolkit will attempt to retrieve the contact Work Phone information and display it here.

##### Email

The toolkit will attempt to retrieve the contact Work Email information and display it here.

##### Site ID

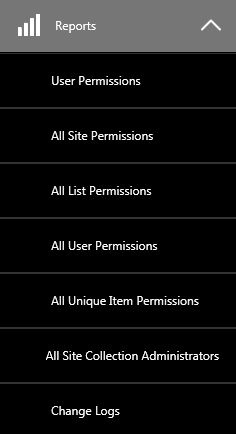
This is the GUID identifier for the Site Collection.

##### SP Version

This is the SharePoint version of the site in the report.

### Merged Reports

From the “Security” button in the Top Navigation, and then under “Reports” in the Left Navigation, you will find “Merged” reports that you may further customize. These reports will show a “Merged” report of all permission reports created for the sites you manage in one view.



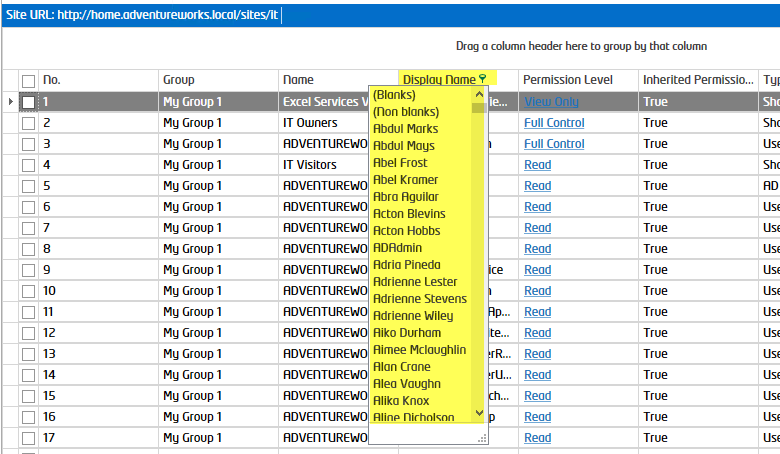
* “User Permissions”: This report combines all “Check User Permissions” reports into one view. This will show all permission objects across farms, web applications, site collections and sites (from reports that have been generated).
* “All Site Permissions”: This report combines all existing “Site Permissions” reports into one view. This will show all site-level permission objects across farms, web applications, site collections and sites (from reports that have been generated).
* “All List Permissions”: This report combines all existing “List Permissions” reports into one view. This will show all list-level permission objects across farms, web applications, site collections and sites (from reports that have been generated).
* “All Unique Item Permissions”: This report combines all existing “Unique Item Permissions” 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).
* “All Site Collection Administrators”: This report combines all existing “Site Collection Administrators” reports into one view. This will show all Site Collection Administrators across farms, web applications, site collections and sites (from reports that have been generated).
* “Change Logs”: This is not a report, it shows the history of changes made using the tool to Site, List or Item permissions.

## Customizing the Report

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

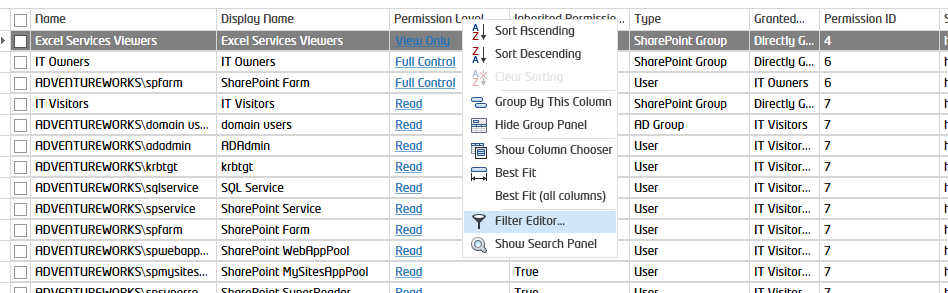
### Filtering

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

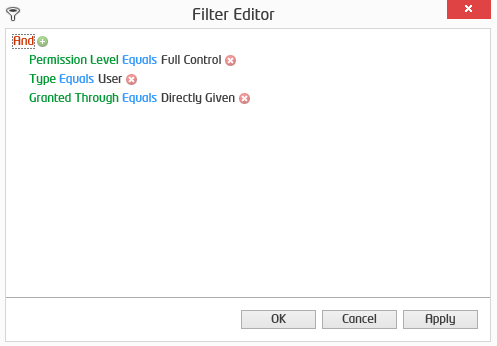


### Advanced Filtering

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



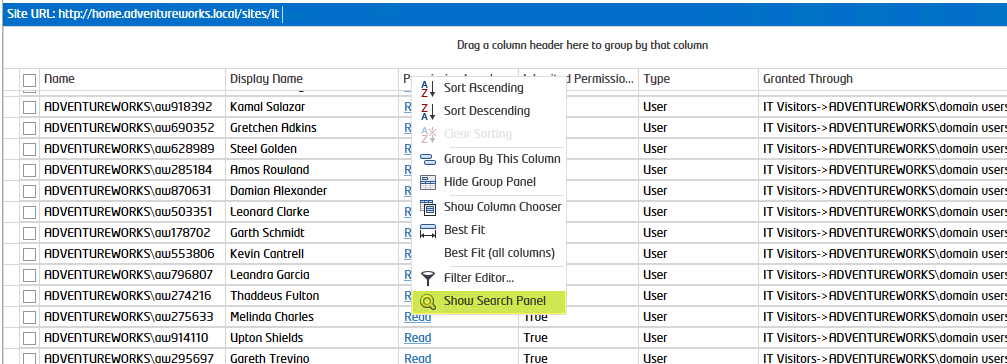
Below is an example of filtering a View to display all areas where a User has been Granted Access directly and has Full Control:



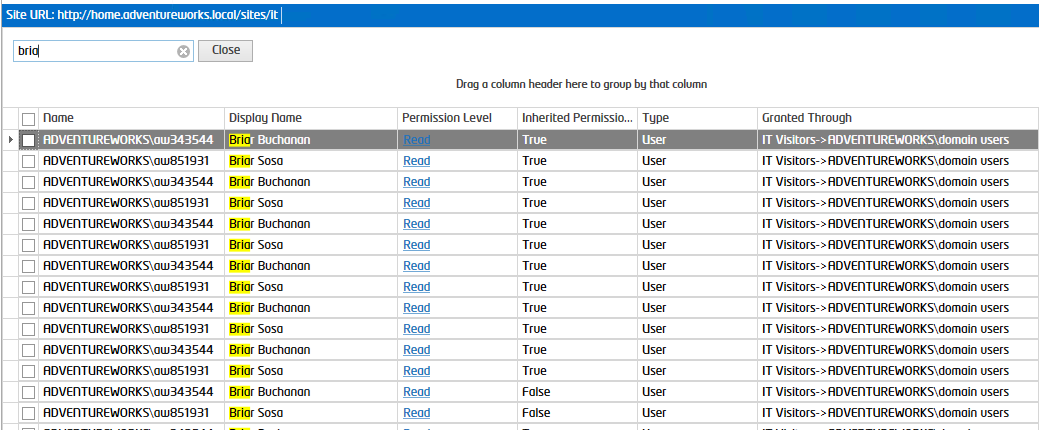
You can apply filters like this and then click “Save View” to re-use for later in other reports.

### Searching within the Report

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



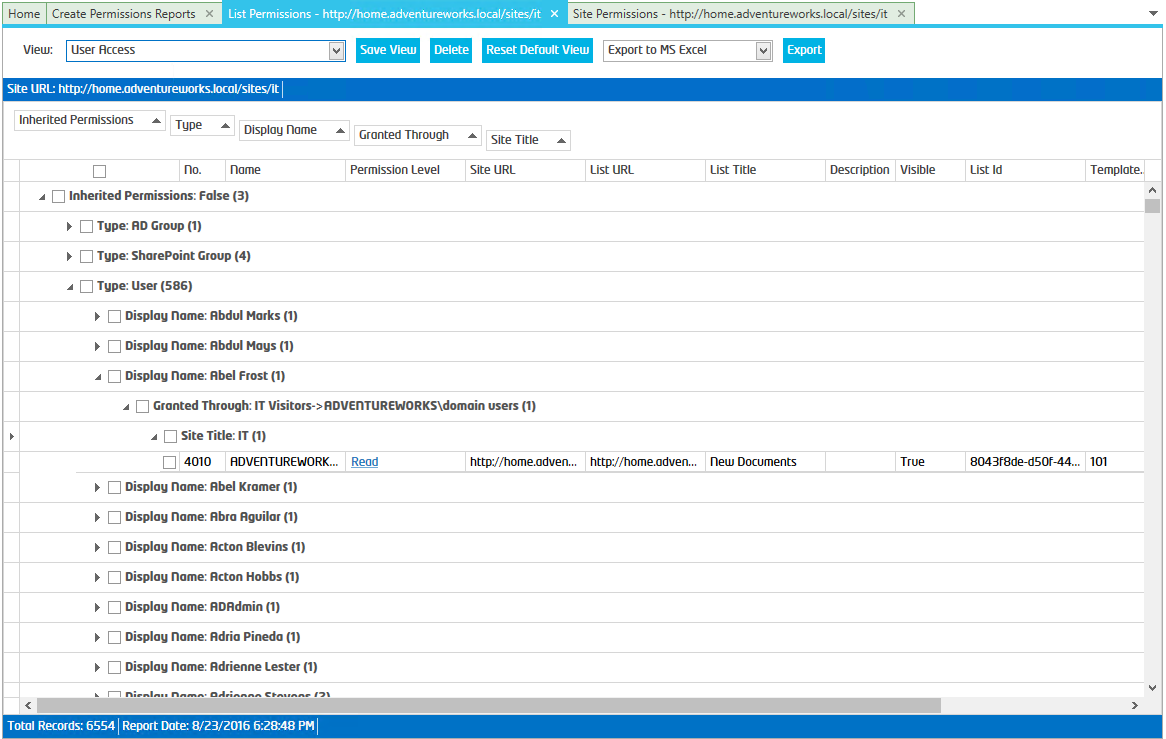
Below I entered “Bria” in the search box and the toolkit will automatically filter results and highlight them yellow.



### Grouping

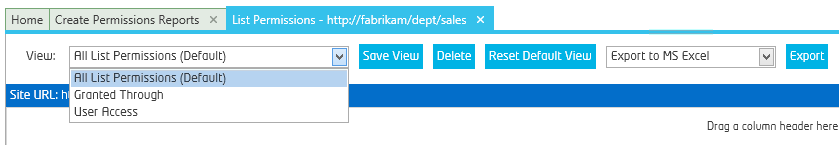
To group the results, drag the column header of the field you want to group by to the top of the results panel. You can also drag multiple panels and rearrange the group ordering by dragging columns left and right of each other

Below I grouped by “Inherited Permissions”, so here I can see all permissions found that are “Unique” and are “Users”:



### Views

The user can save views or modify the default view by clicking “Save View”. A view can be deleted by clicking “Delete”, the user will be prompted to delete the current view. The Default view cannot be deleted. “Reset Default View” will reset the Default view to the ‘out of the box’ view.

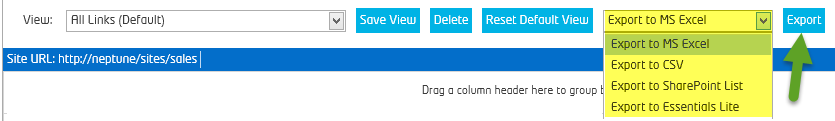


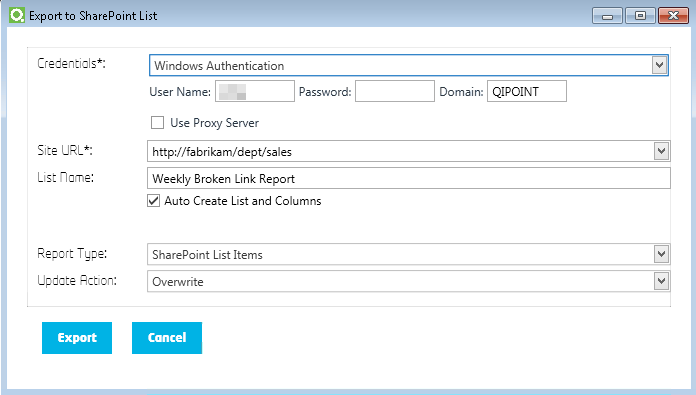
### Export

A report can be exported to the following formats directly:

1. MS Excel
2. CSV
3. SharePoint List
   1. As SharePoint List Items
   2. Uploaded as MS Excel File
   3. Uploaded as QPCX File (SharePoint Essentials Lite Client)
4. QPCX (SharePoint Essentials Lite Client)

To perform the export, select the option in the drop down and then by clicking the “Export” button. Alternatively, multiple rows can be highlighted and ‘Copied’ by right clicking and selecting “Copy”. Then the selected rows can be pasted in MS Excel, an Email, MS Word or any compatible program.





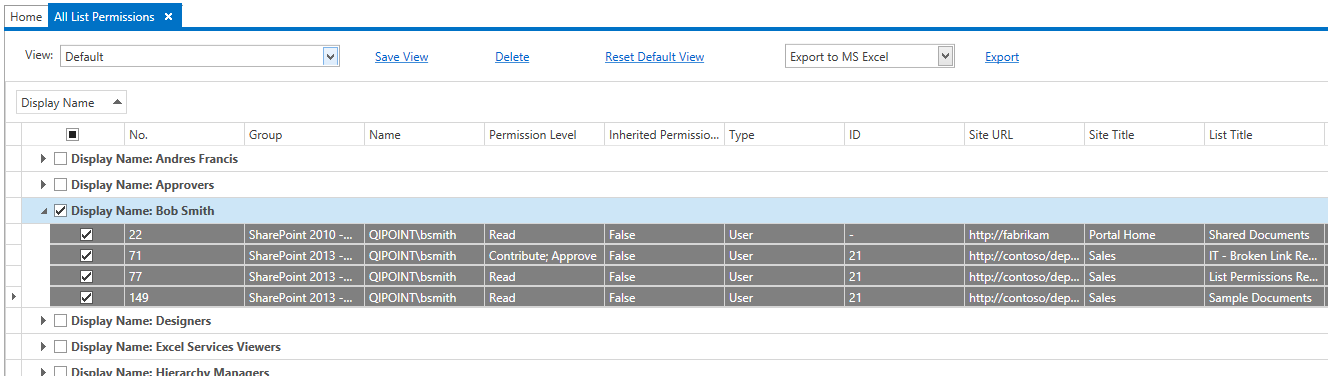
# Permission Templates – “Save Job”

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

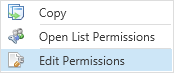
To do this:

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’

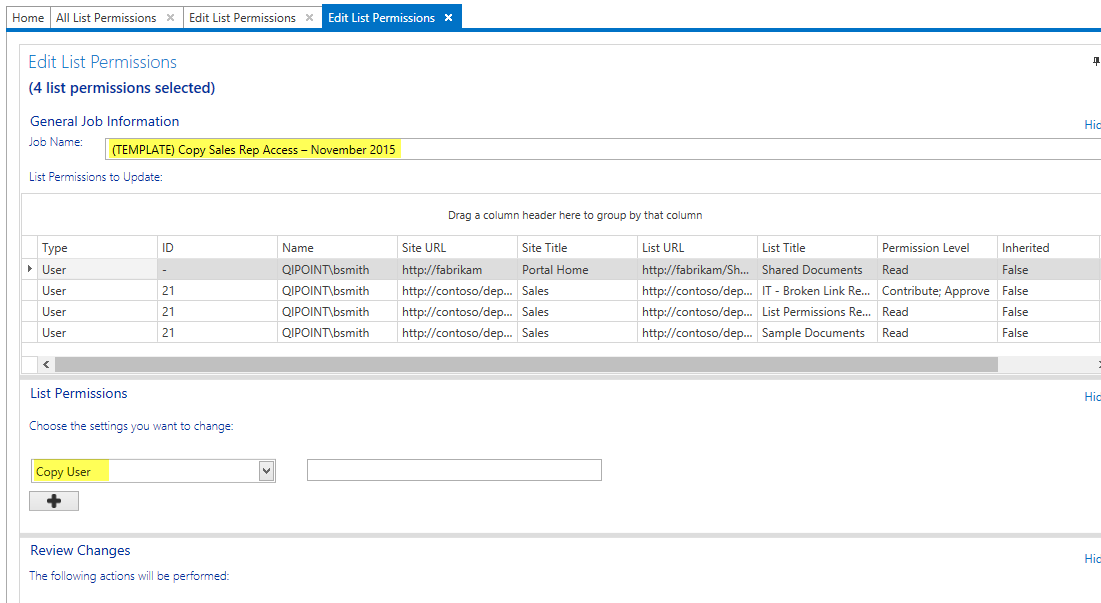
For example, if a user needs to grant access to other users based on Bob Smiths access (perhaps he is a Sales Rep and I often need to duplicate his access to others), I would select his permission objects as done below: (in this simple example Bob Smith only has unique access to 4 lists)



1. Right click and select “Edit Permissions”

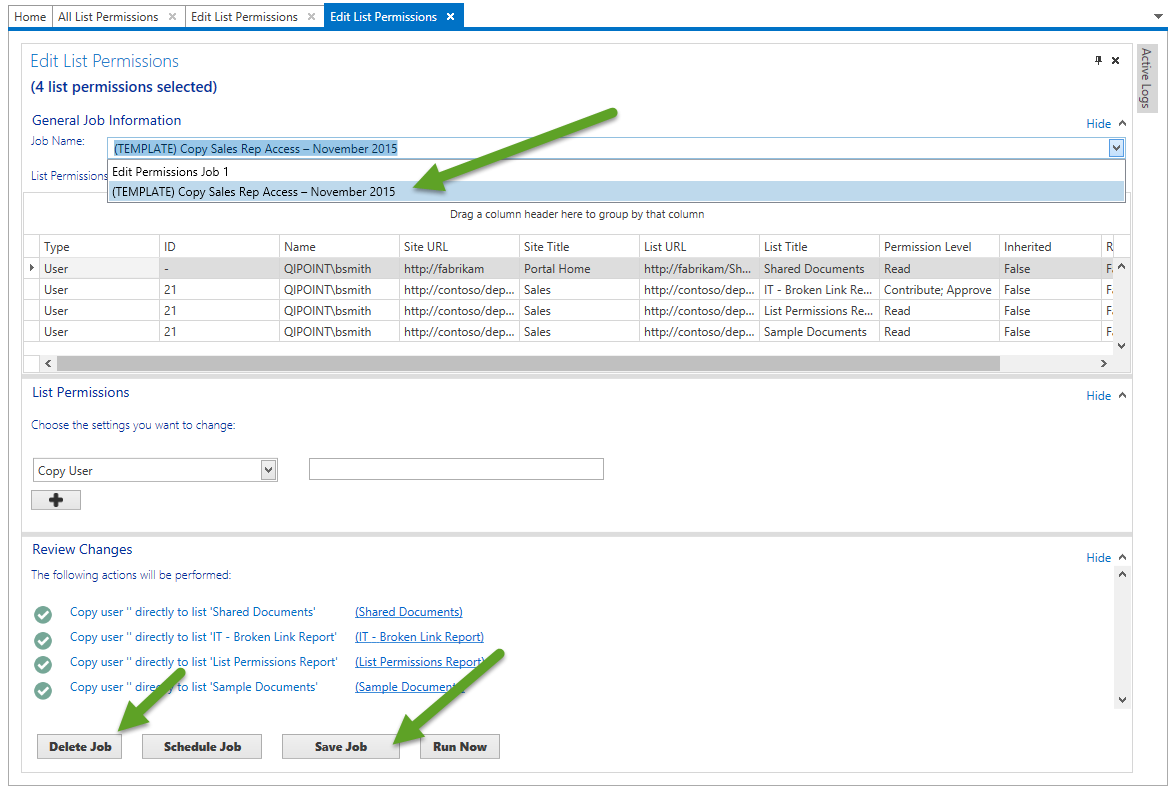


1. The Edit List Permissions window will open (or whichever appropriate window based on the permission template being created, such as Edit Site Permissions)
2. Enter a unique Job Name for the ‘template’, such as “(TEMPLATE) Copy Sales Rep Access”



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.



# Manage

## Editing Permissions

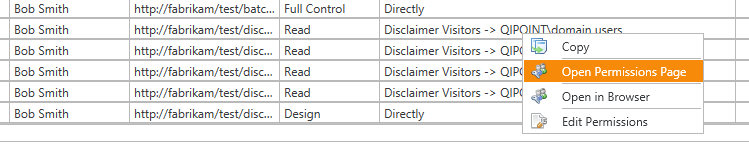
To edit permissions for one or more sites, you first need to run a report on those sites.

You can modify permissions in 2 ways:

1. (Manually) 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.

### 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.

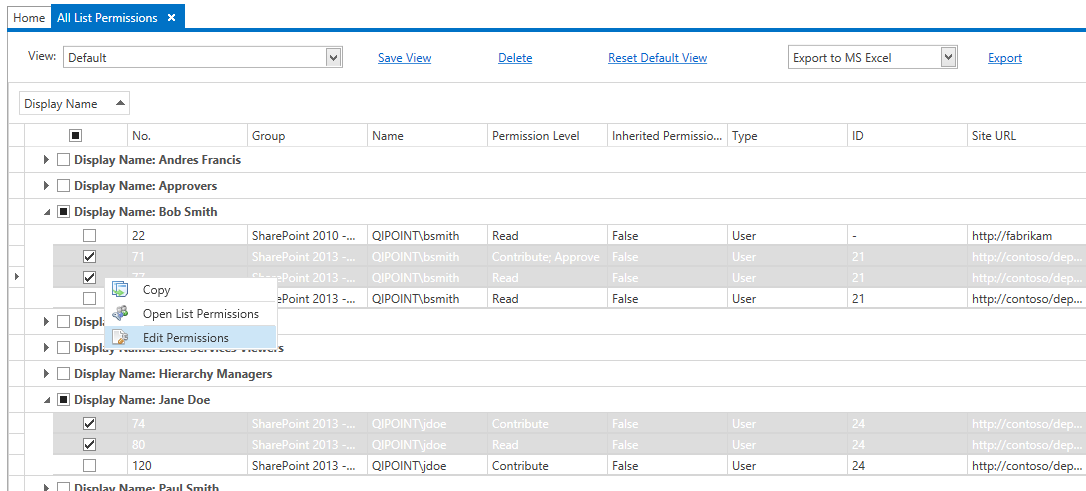


### Automatically Updating User / Group Permissions

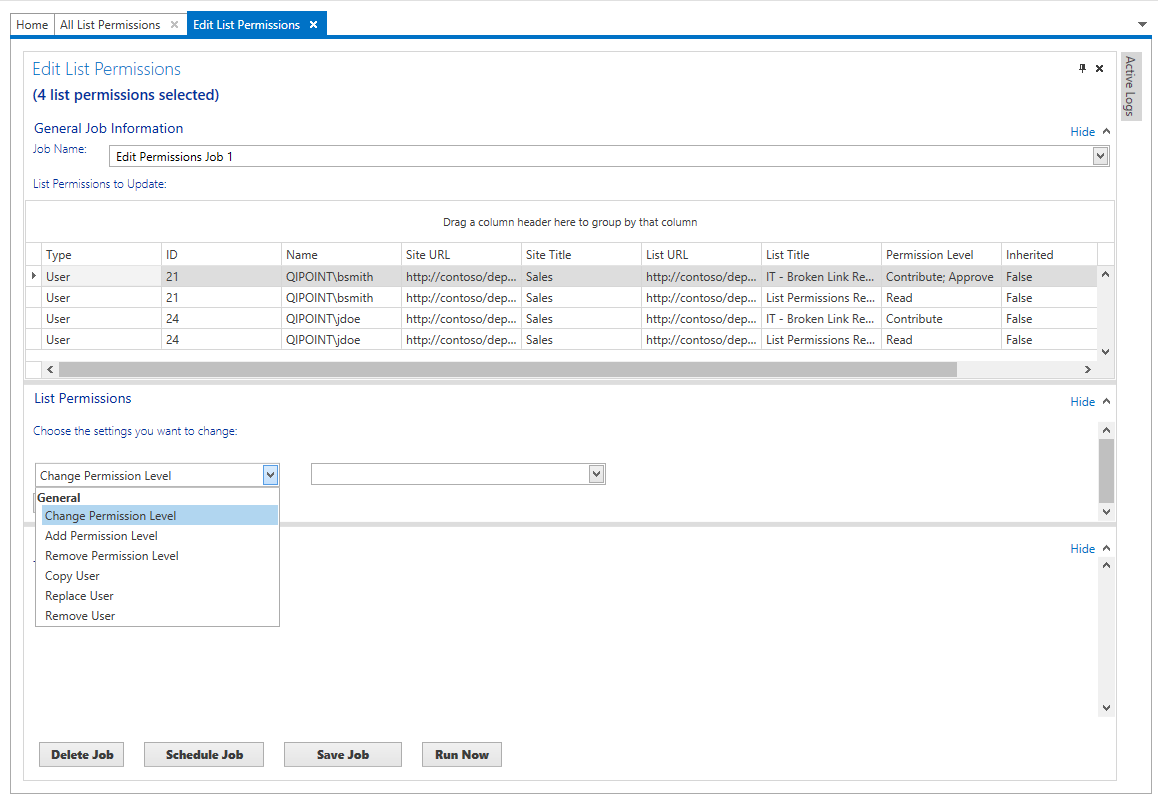
If the user finds a Site or List with permissions that they need to correct:

* From the grid view report Select the permissions you wish to modify (using leftmost checkbox). NOTE: You can only modify ‘non-inherited permissions’ and objects of the same “Type” (such as Users or Groups, not both at the same time)
* 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.



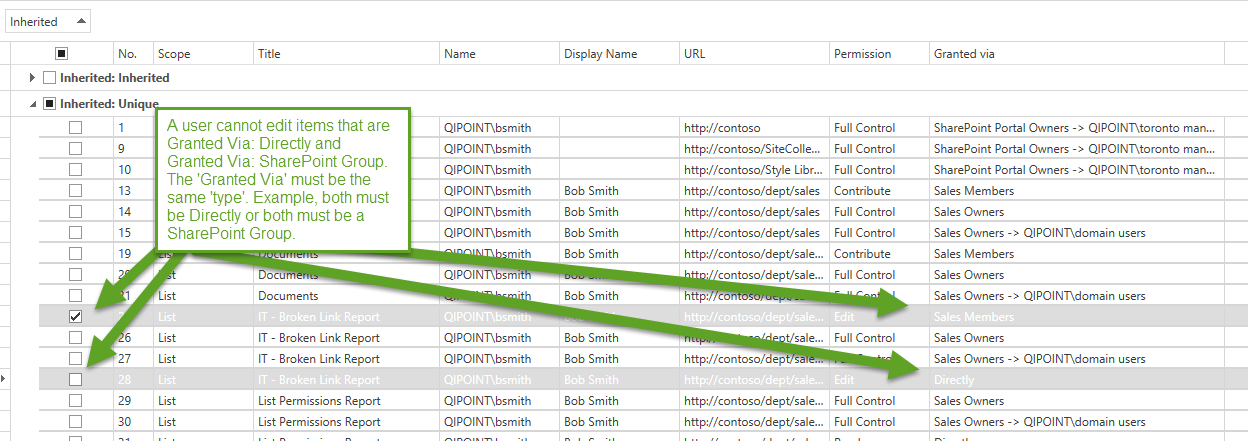
* The Edit Permissions window will open. This is where you can: modify the selected objects permissions, copy the permissions to another user/group, replace the user/group, or just remove access.



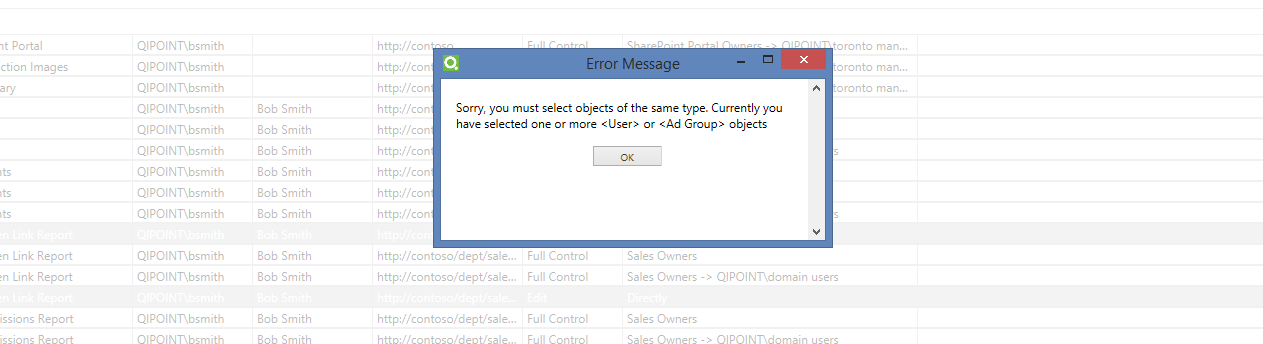
**NOTE**

* 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’.

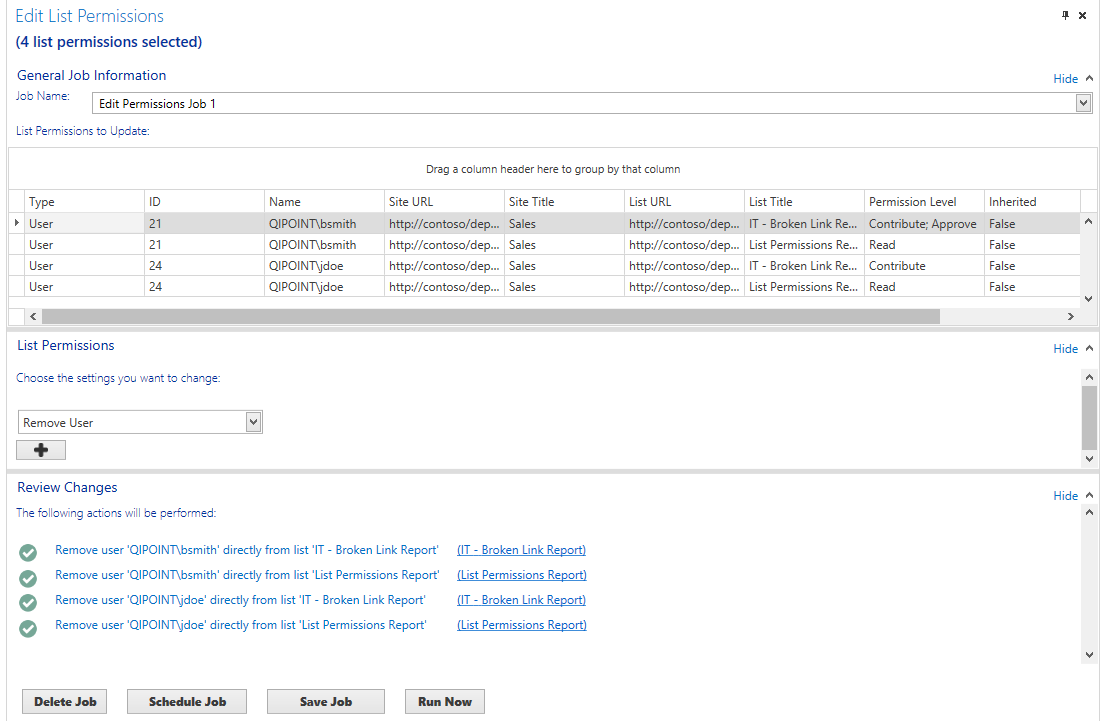
For example, if you have a report with permissions granted for Bob Smith, and one list shows ‘Granted Via: directly’ (which indicates the User’s permission was added ‘directly’ to the list) and another list shows ‘Granted Via: SharePoint Portal Members’ (where the user was granted access by adding the 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:



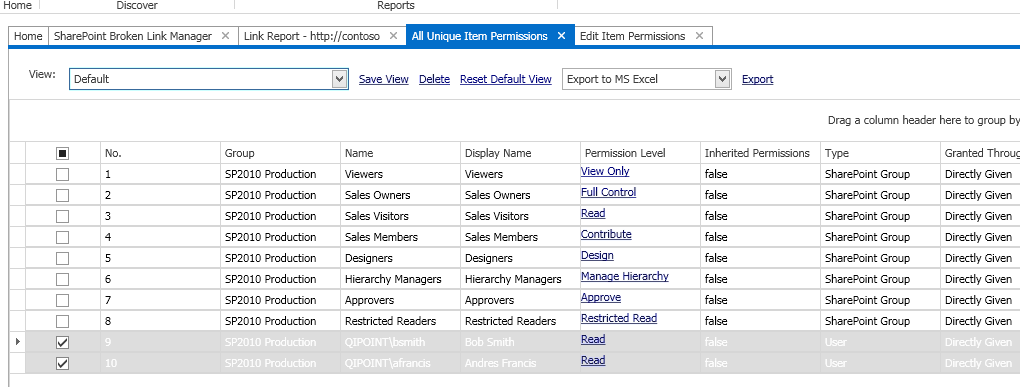
### How to schedule removal of User Accounts (from Site, List or Item Level)

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

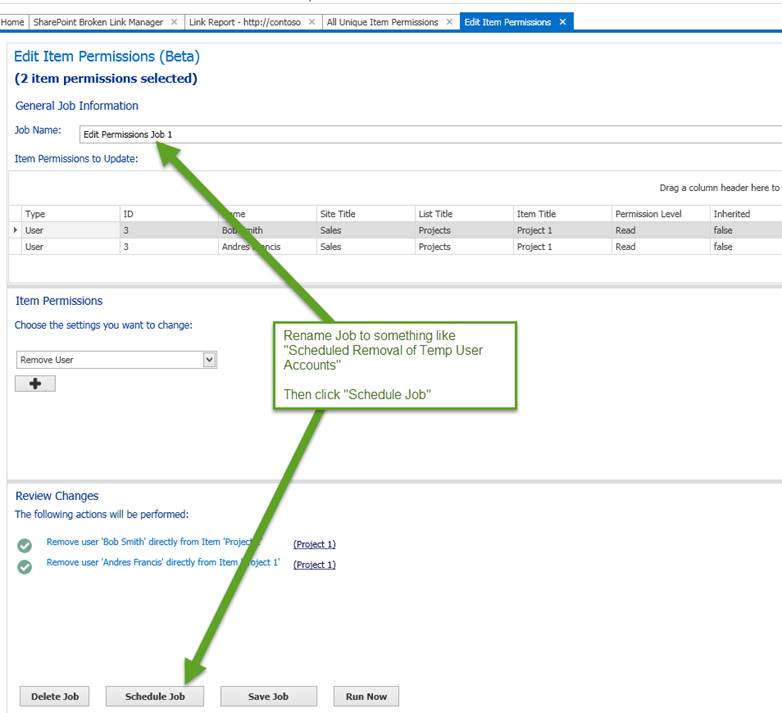
1. First you need to create a Basic Permissions Report for the site to make changes to. The toolkit approach is “Discover, Review, Manage’’.
2. After that is complete, click “All Unique Item Permissions” (or other permissions report button you want to make edits to) from Permissions Left Navigation.
3. Select the users you want to schedule the account removal (TIP: You can group by ‘Inherited Permissions’, ‘Access Type’ and ‘Item Title’ to make it easier to view)

NOTE: You can only modify permissions where “Inherited Permissions = false”.

You can turn on/off Inherited Permissions for multiple sites and/or lists using the Site Auditing Component to modify site and list settings.



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 Jobs

This product includes a built-in scheduler 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).

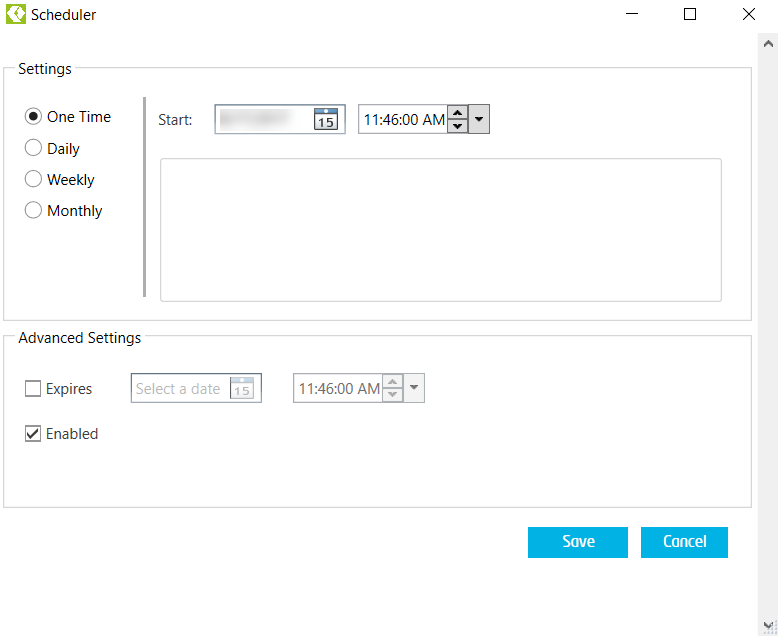
**TIP:** Ensure the “QiPoint Essentials Service” (Windows Service) is running before trying to schedule a job. Ensure the user account used to run the service has ‘Modify’ permission to the Report Path (Home->Settings). By default, this service uses ‘Local System’ which may not have rights to create files (reports) in a network file share for example.



## 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.

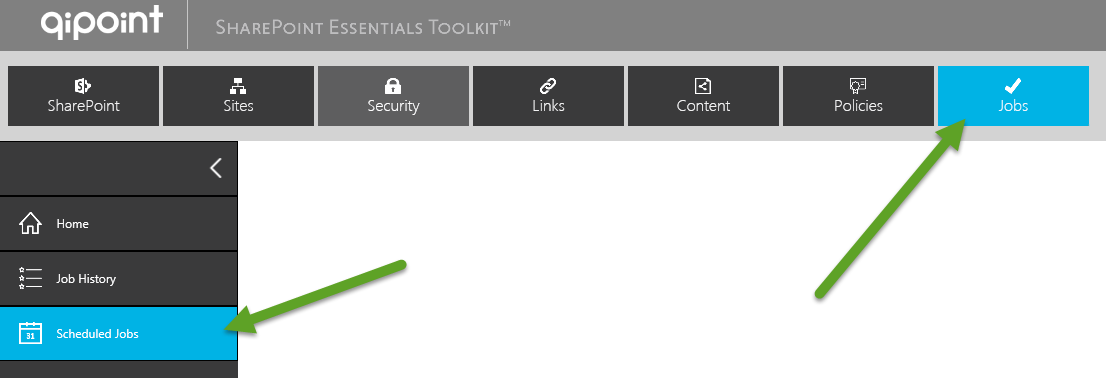


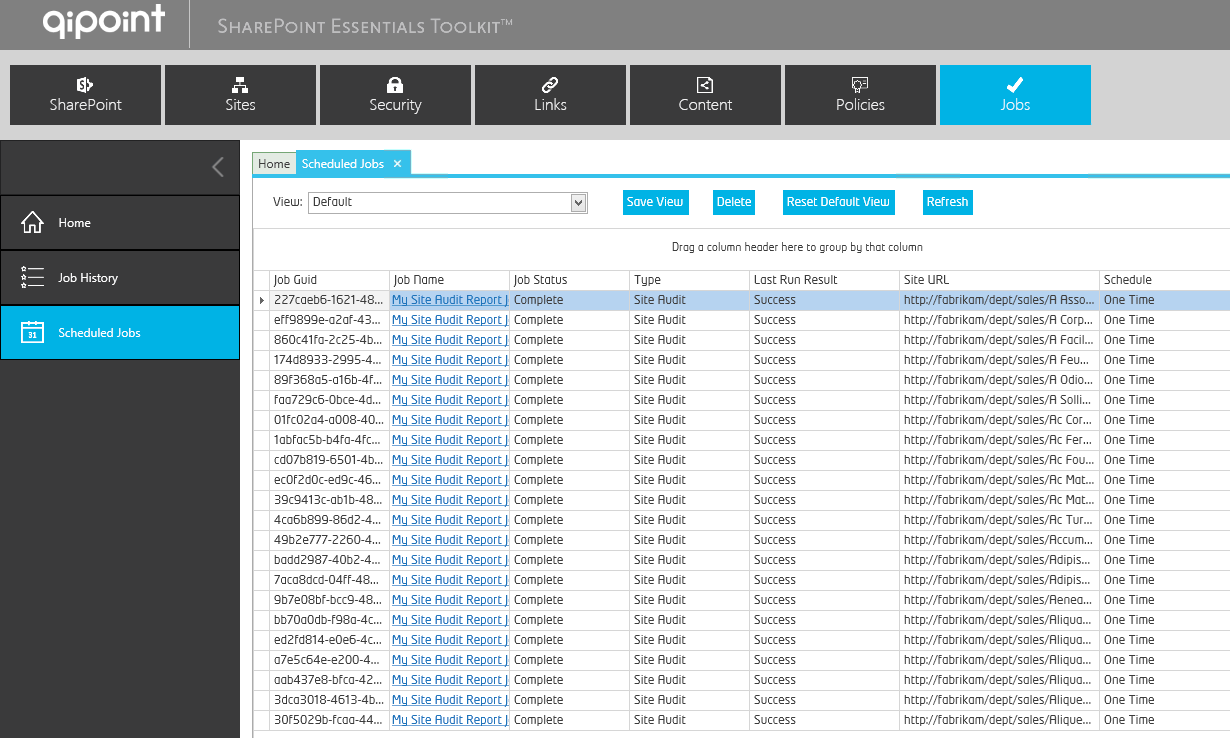


Select the schedule and specific options and click OK to save the scheduled job.

## List of Scheduled Jobs

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





From here you can view reports, logs, execute the job, modify or delete scheduled jobs (by right clicking the job).

## Scheduled Job Logs and Reports

After a Scheduled Job is complete, you can right click it to view the logs or the actual reports. You can also access these logs and reports from the Home Page Dashboard, and also from the Job History section of the tool.

NOTE: Only applicable reports and logs will be shown.



# 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.

# 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).

# 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)

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

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

We are here to help!

# Product Features

|  |  |
| --- | --- |
| Feature | Enterprise |
| Scan SharePoint 2010 |  |
| Scan SharePoint 2013 |  |
| Scan SharePoint 2016 |  |
| 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 SharePoint Group Nested Permissions |  |
| Include AD Group Nested Permissions |  |
| Hide Limited Access in Reports |  |
| Report Specific User or Group Permissions |  |
| Export to MS Excel |  |
| Grouping of Scan Results in grid |  |
| Save custom Report Views |  |
| 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 |  |