|  |
| --- |
|  |
| SharePoint Permissions Manager™ |
| User Manual |
|  |
|  |
| **Last updated: 10/20/2022** |

|  |
| --- |
|  |

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

Table of Contents

[Introduction 4](#_Toc21100637)

[Installation & Minimum Requirements 5](#_Toc21100638)

[IMPORTANT: This program does not need to be installed on a SharePoint Server. 5](#_Toc21100639)

[Minimum Hardware Recommendations 5](#_Toc21100640)

[Supported SharePoint Versions 6](#_Toc21100641)

[.NET Framework Required 6](#_Toc21100642)

[Local Machine & Windows System Permissions Required 8](#_Toc21100643)

[Anti-Virus, Offline Sync Folders (i.e. Google Drive, OneDrive, Drop Box, etc.) and Performance 8](#_Toc21100644)

[SharePoint User Permissions Required 9](#_Toc21100645)

[Azure Active Directory Groups and Members 9](#_Toc21100646)

[Permissions needed to generate Permission Reports 9](#_Toc21100647)

[Note when using Least Privileged Approach 10](#_Toc21100648)

[Required Permissions to use the “Edit Permissions” bulk function 10](#_Toc21100649)

[Office 365 Accounts 10](#_Toc21100650)

[Permission Report Limitations and Notes 11](#_Toc21100651)

[Web Application User Policy Permissions 11](#_Toc21100652)

[Getting Started 12](#_Toc21100653)

[Build your First Permissions Report 13](#_Toc21100654)

[Method 1: Use the Home Page Dashboard to build a permissions report 13](#_Toc21100655)

[Method 2: Use Security Tab to build a permissions report 16](#_Toc21100656)

[Report Options 20](#_Toc21100657)

[Job Name\* 20](#_Toc21100658)

[Site URL to Scan\* 20](#_Toc21100659)

[Hide Limited Access 21](#_Toc21100660)

[Site Collection Administrators 21](#_Toc21100661)

[SharePoint Groups 21](#_Toc21100662)

[Site Permission 21](#_Toc21100663)

[List Permission 22](#_Toc21100664)

[Unique Item Permission 22](#_Toc21100665)

[Show Nested Permissions (SP Groups) 22](#_Toc21100666)

[Show Nested Permissions (Domain Groups) 23](#_Toc21100667)

[Open Report 24](#_Toc21100668)

[Credentials 24](#_Toc21100669)

[Email (Optional) 25](#_Toc21100670)

[Inclusion Rules 26](#_Toc21100671)

[Exclusion Rules 26](#_Toc21100672)

[Report Export Options 28](#_Toc21100673)

[Discover (section in Left Navigation) 31](#_Toc21100674)

[Reports (section in Left Navigation) 32](#_Toc21100675)

[Check User Permissions Reports 36](#_Toc21100676)

[How to Create a User Permissions Report 36](#_Toc21100677)

[*Inclusion Rules (Optional)* 40](#_Toc21100678)

[*Exclusion Rules (Optional)* 40](#_Toc21100679)

[NOTE: Inclusion/Exclusion Rules: 41](#_Toc21100680)

[Export Options (Optional) 42](#_Toc21100681)

[Check Orphaned Users 45](#_Toc21100682)

[How to Create an Orphaned Users Report 45](#_Toc21100683)

[Show Advanced Options 47](#_Toc21100684)

[Logs 52](#_Toc21100685)

[Physical Log files and reports 52](#_Toc21100686)

[Export Logs 53](#_Toc21100687)

[Opening Reports / Viewing Historical Reports 54](#_Toc21100688)

[Open report for current Job 54](#_Toc21100689)

[Past Jobs / Historical reports 54](#_Toc21100690)

[How to Interpret the Reports 57](#_Toc21100691)

[Interpreting the Reports 57](#_Toc21100692)

[Opening the Report 58](#_Toc21100693)

[Customizing Permission Reports 75](#_Toc21100694)

[Filtering 75](#_Toc21100695)

[Advanced Filtering 75](#_Toc21100696)

[Searching within the Report 76](#_Toc21100697)

[Grouping 77](#_Toc21100698)

[Creating “Views” 78](#_Toc21100699)

[Export 79](#_Toc21100700)

[Permission Templates – “Save Job” 80](#_Toc21100701)

[Updating Permissions 82](#_Toc21100702)

[Editing Permissions 82](#_Toc21100703)

[Manage Permissions: Manually via SharePoint 82](#_Toc21100704)

[Manage Permissions: Using SharePoint Essentials Toolkit 83](#_Toc21100705)

[Scheduling Jobs 86](#_Toc21100706)

[Schedule a Job 86](#_Toc21100707)

[List of Scheduled Jobs 88](#_Toc21100708)

[Scheduled Job Logs and Reports 88](#_Toc21100709)

[Report Archive 90](#_Toc21100710)

[Technical Support 91](#_Toc21100711)

[Product Features 91](#_Toc21100712)

# 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:

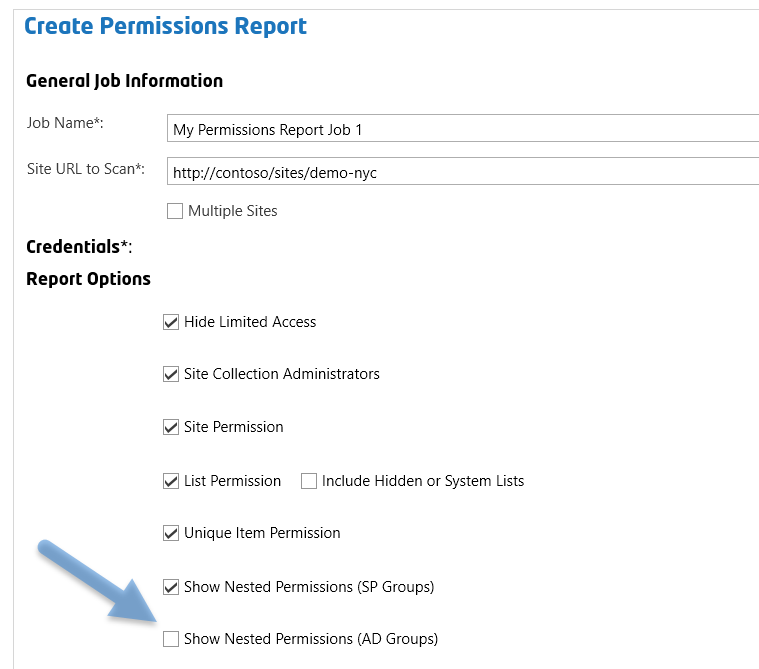
* At least 1GB of available RAM for jobs\* with less than 1,000 uniquely permissioned objects
* At least 2GB of available RAM for jobs\* with less than 5,000 uniquely permissioned objects
* At least 4GB of available RAM for jobs\* with less than 100,000 uniquely permissioned objects
* At least 6GB of 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 (refreshed every job but does not lookup same AD Group or SharePoint Group with same ID twice) to improve performance (vs. re-fetching all 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 (Domain Groups)”**

Use this option 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 members within each of these two groups. In many organizations, this number (number of members) can be in tens of thousands, and in some case’s more, 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.



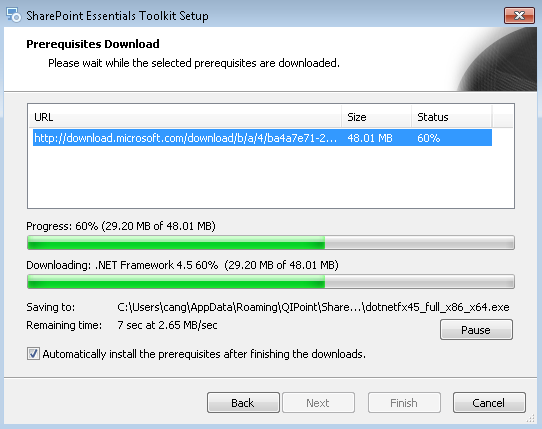
**Hard Disk:** 300MB Available Hard Disk Space (for the application files, logs, temp files and reports).   
Temp files are automatically cleared as needed. This is in addition to the disk space required by the SharePoint Essentials Toolkit.

## Supported SharePoint Versions

Microsoft SharePoint Online / Office 365  
Microsoft SharePoint Server 2019  
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. Users do not require Full Control or Farm/Site Collection Administrator rights, they only require Read Rights with the addition of ‘Enumerate Permissions’ as indicated below.

## Azure Active Directory Groups and Members

Microsoft Azure Active Directorygroupmembers can be displayed in reports using this tool. However, this feature requires an Office 365 Global Administrator grant access to the SharePoint Essentials Toolkit (2 step process). For more information about the consent required, please visit: <https://www.cognillo.com/sharepoint-essentials-toolkit-consent>. Once consent is provided, users can generate reports with the permission below to view Azure AD Group members.

## Permissions needed to generate Permission Reports

Providing the permission levels below will allow a user to use the tool to build permissions reports using the SharePoint Essentials Toolkit. The permissions below are equivalent to READ + Enumerate Permissions permission levels.

**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 for accessing items inside that container.

**NOTE: T**he above permission levels are required for each site you will run the report for. If the report is being run for a subsite, the account running the tool will require Read permission on the root site.

## Note when using Least Privileged Approach

When following best practices and attempting to use a ‘least-privileged’ approach to granting rights to generate reports, keep in mind that users can generate permission reports using the SharePoint Essentials Toolkit with only **Read + Enumerate** **Permissions**, however, if this permission is granted to users (who will use the tool to build reports) at the site level, if Lists and/or folders or files have unique permissions which the user does NOT have **Read + Enumerate Permissions**, the user will see a warning in the logs that one or more lists/items could not be accessed, and these lists and items will not appear in the report(s). In this case, we recommend to use an account that is a member of the Site Collection Administrators (or at tenant/farm/web application level) to run the report.

## Required Permissions to use the “Edit Permissions” bulk function

The account will require **Manage Permissions** permission level if the user would like to use the ‘Edit Permissions’ option.

## Office 365 Accounts

* When managing 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.

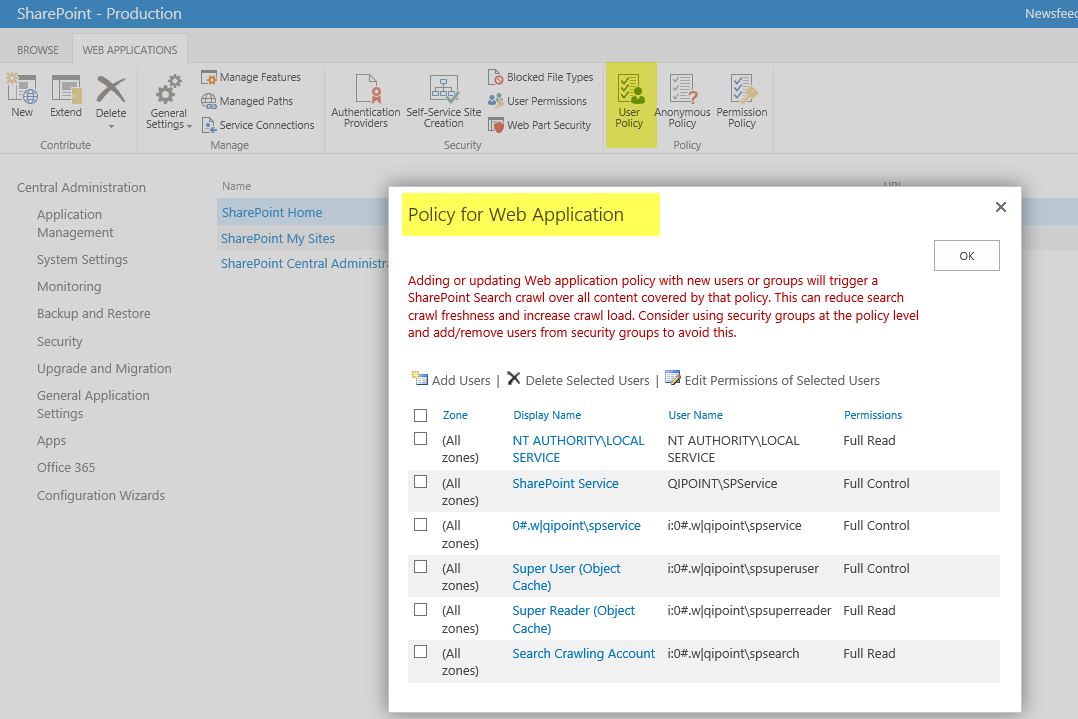
# Permission Report Limitations and Notes

* 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 and are not shown in these 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 (Domain Groups)’ is selected, the tool will show all active (not disabled) AD Accounts.
* (SharePoint Online only) Global Administrators and SharePoint Administrators assigned in the Tenant Administration portal are not displayed in the reports.
* (SharePoint Online only) An Office 365 Global Administrator must consent to allow Azure Active Directory members to be retrieved using the SharePoint Essentials Toolkit. For more information on this, please visit <https://www.cognillo.com/sharepoint-essentials-toolkit-consent>

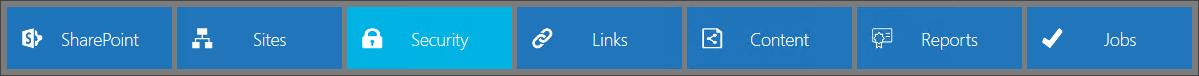
## Web Application User Policy Permissions

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)



# Getting Started



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

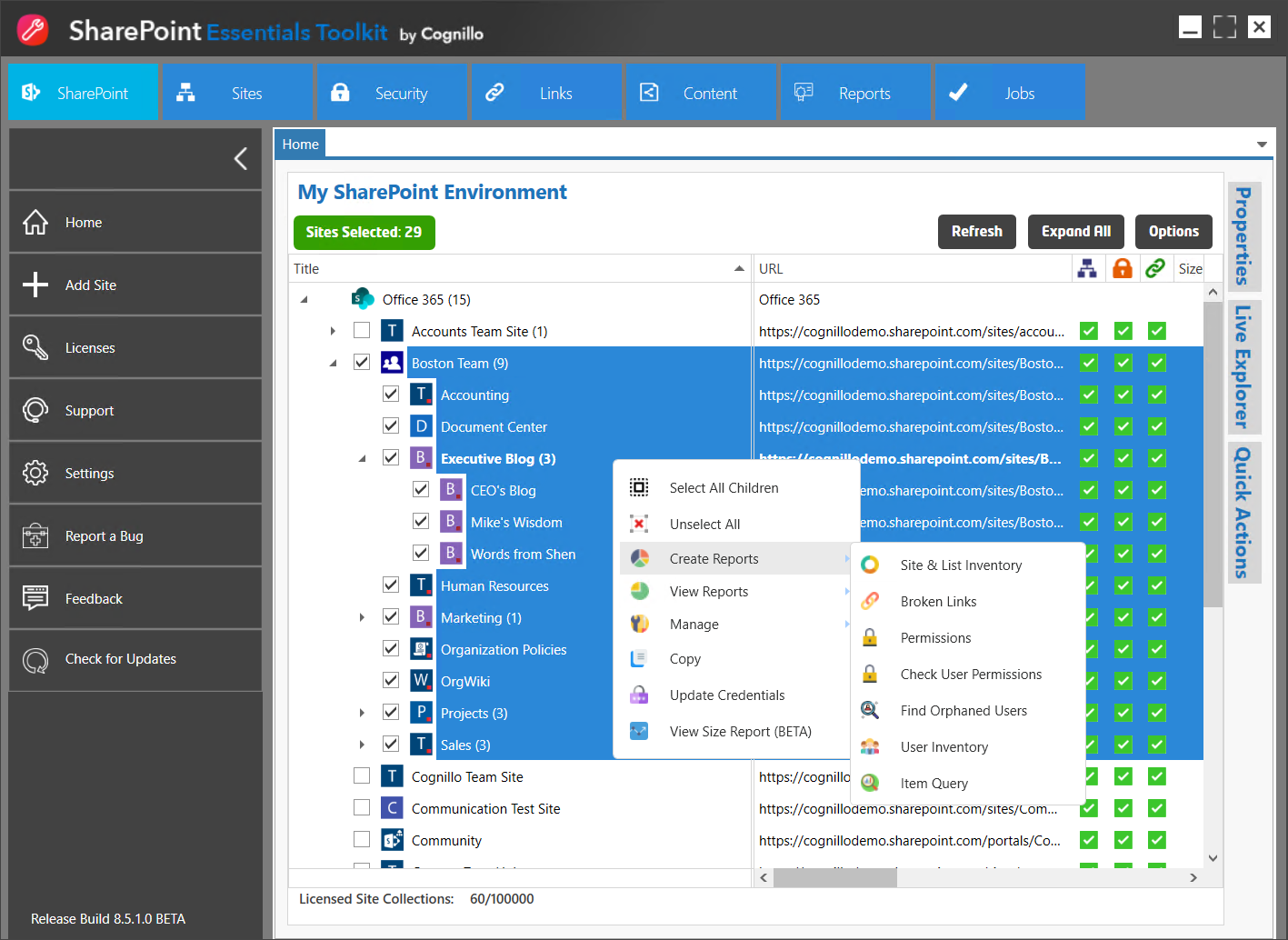
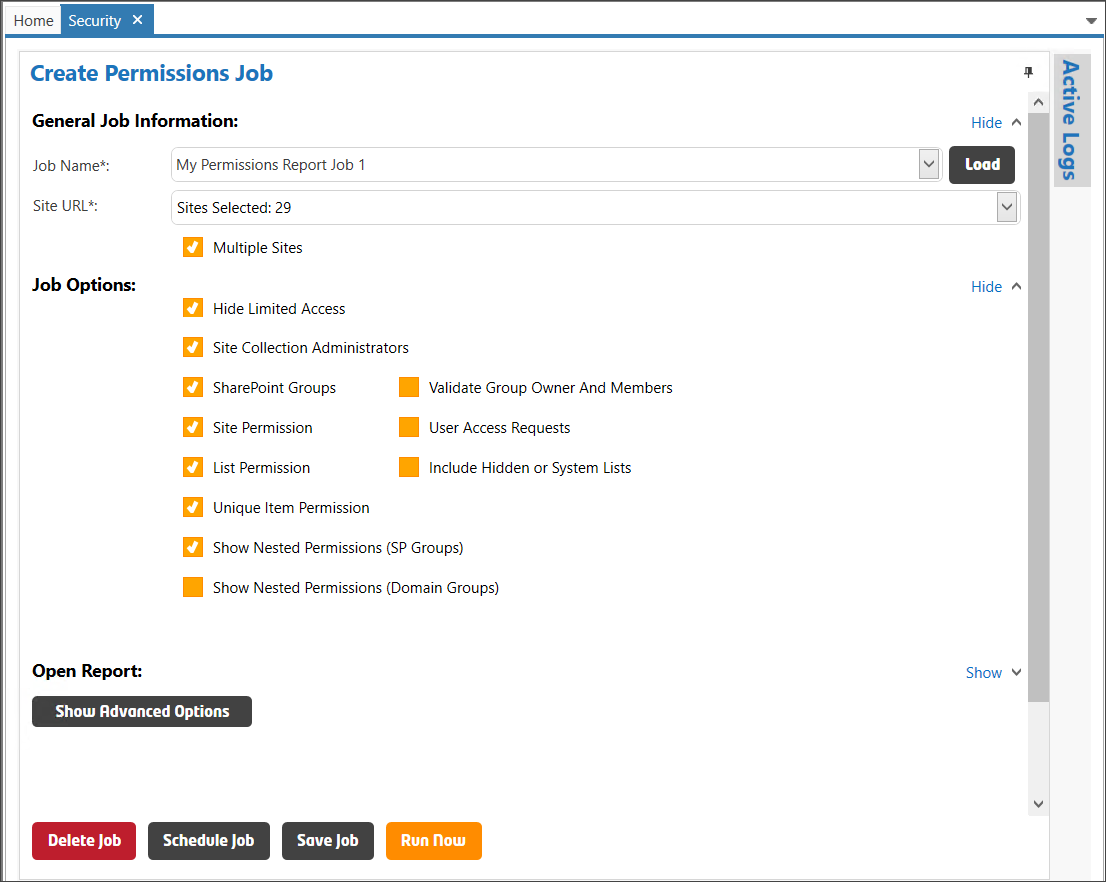
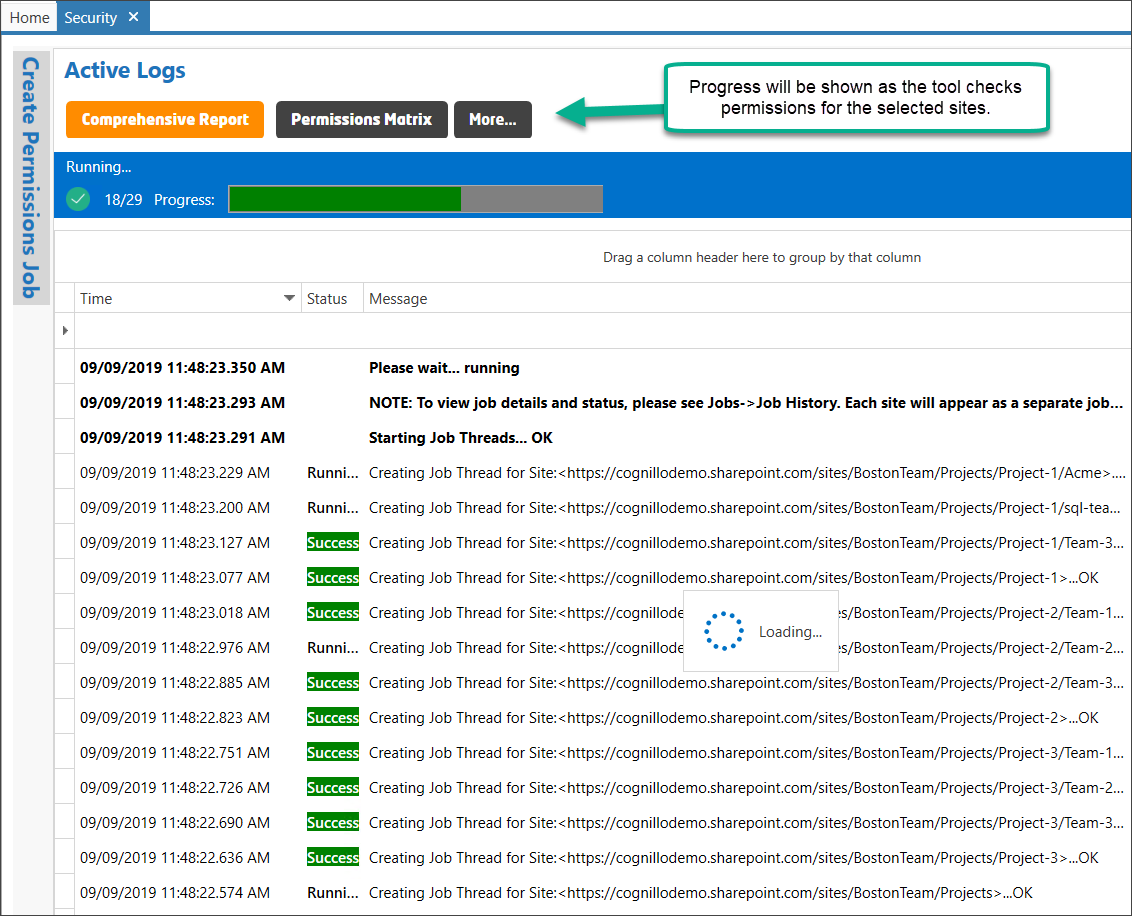
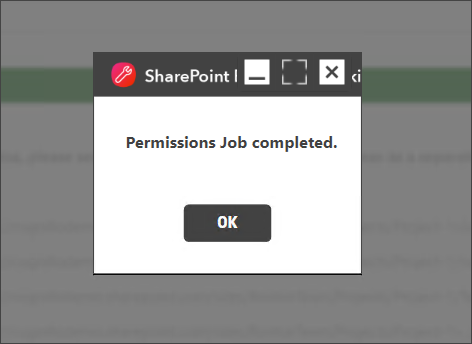
The tool works with the process: “Discover, Analyze, Manage”

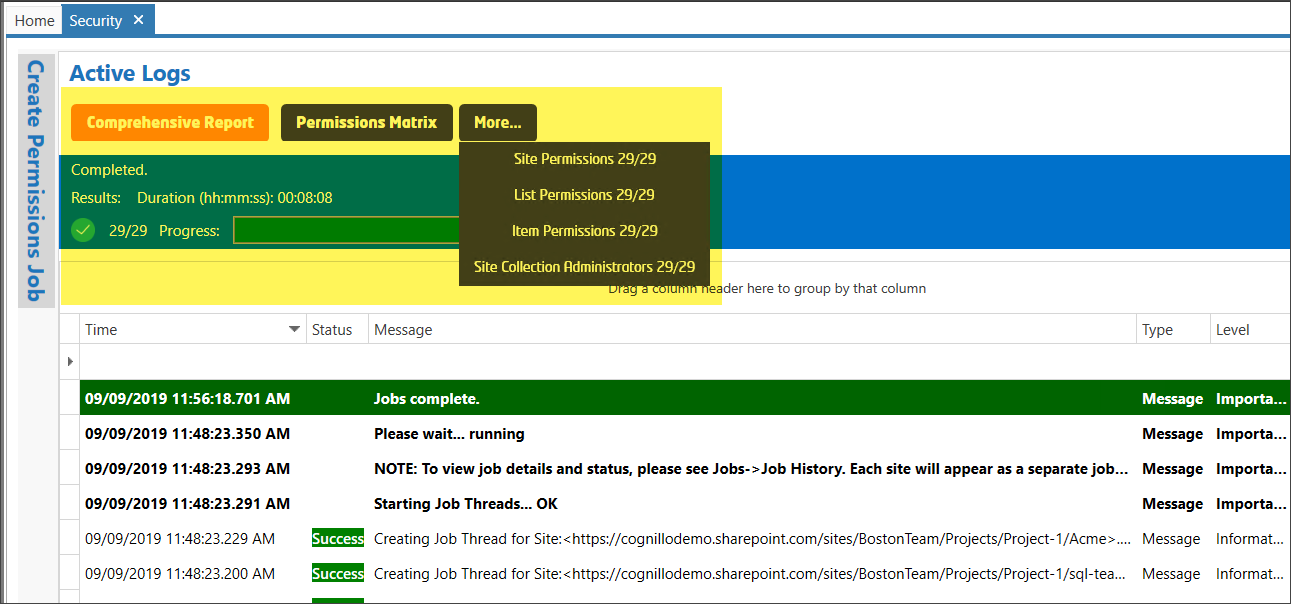
## Build your First Permissions Report

The first thing you need to do, is to add sites to your Home Page Dashboard. You can do this by clicking “Add Site” in the left navigation. **See the “SharePoint Essentials Toolkit – Installation & Deployment Guide”** [**here**](https://www.cognillo.com/user-manuals) **for more information about this.**

There are two ways you can build a SharePoint Permissions report:

### Method 1: Use the Home Page Dashboard to build a permissions report

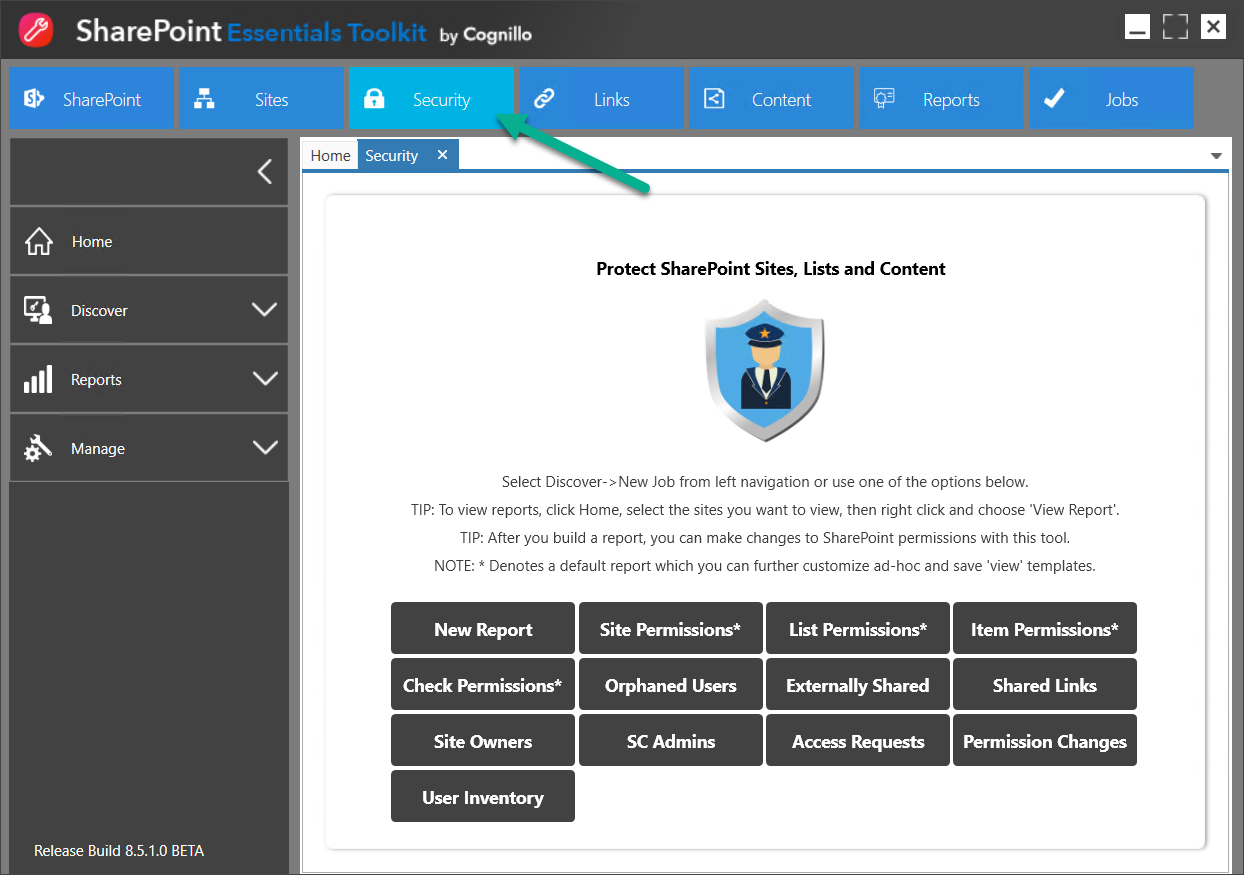
1. Select the sites from the Home Page Dashboard you want to report on:  
     
   
2. Right click, and select Create Reports -> Permissions
3. You will be presented with the Report Options page:  
     
   
4. The “Site URL” will show the number of sites selected to include in the permissions report. You can click the drop down to modify the sites to include if needed.
5. Select the reports and options to include.   
   See “[Job Options](#_Job__Options)” section for information about each option.
6. Click “Run Now”
7. Active Logs page will open to show you job progress  
     
   
8. You can minimize the tool and the job will continue to run. Once complete, you will be notified:  
     
   
9. Select one of the report buttons/links to open one of the Permission reports:



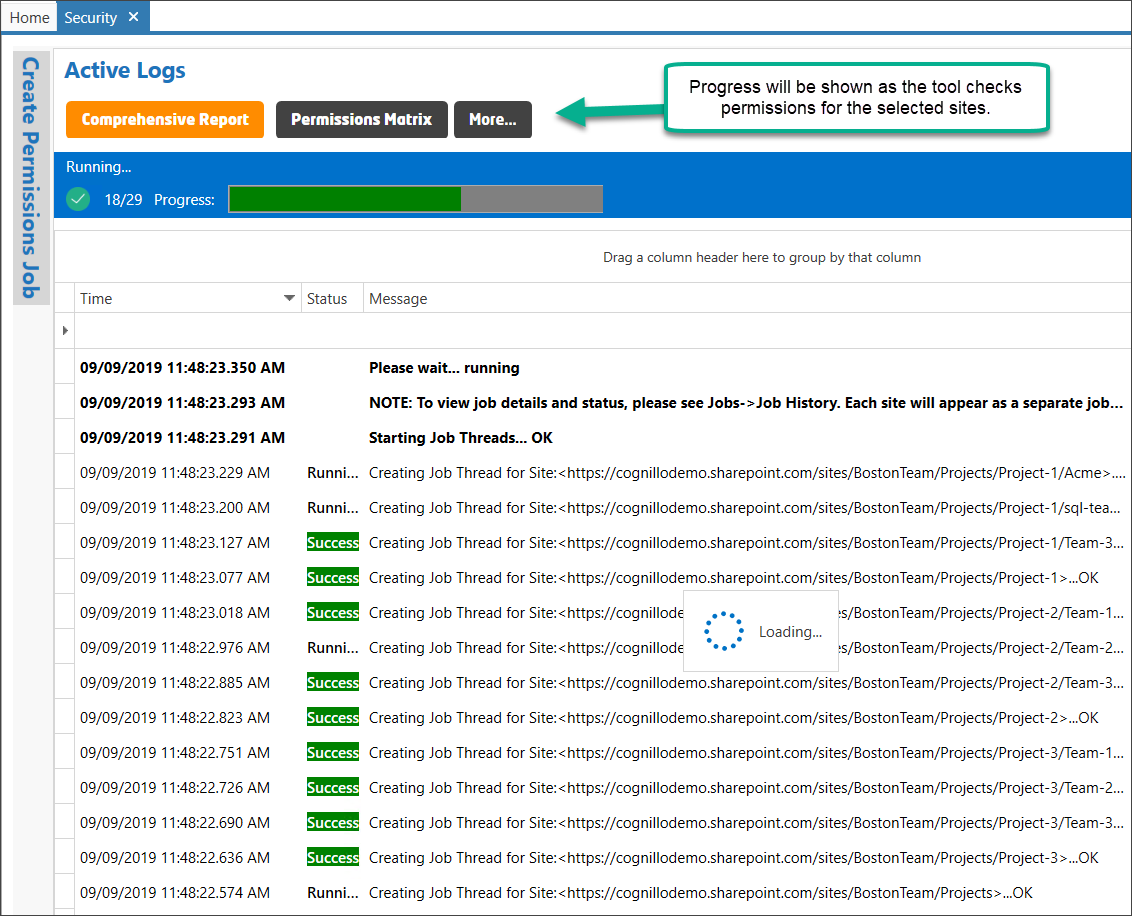
### Method 2: Use Security Tab to build a permissions report

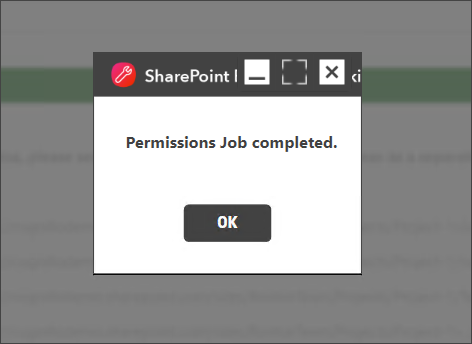
You can create ‘canned’ or ‘ad-hoc’ permission reports from the Security section of the tool.

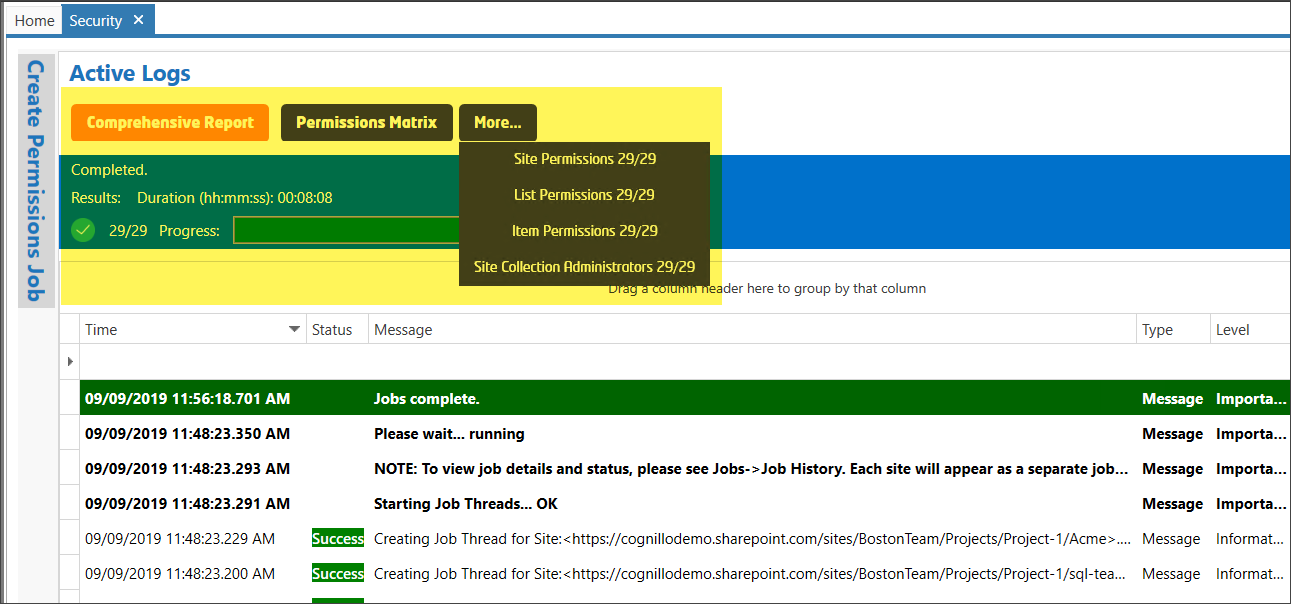
1. Click “Security” button in the top navigation.
2. You will see the Security welcome page below:



1. From here, you can click on any of the buttons to build the appropriate Permissions report.
2. Select the reports and options to include.   
   See “[Report Options](#_Job__Options)” section for information about each option.
3. Click “Run Now”

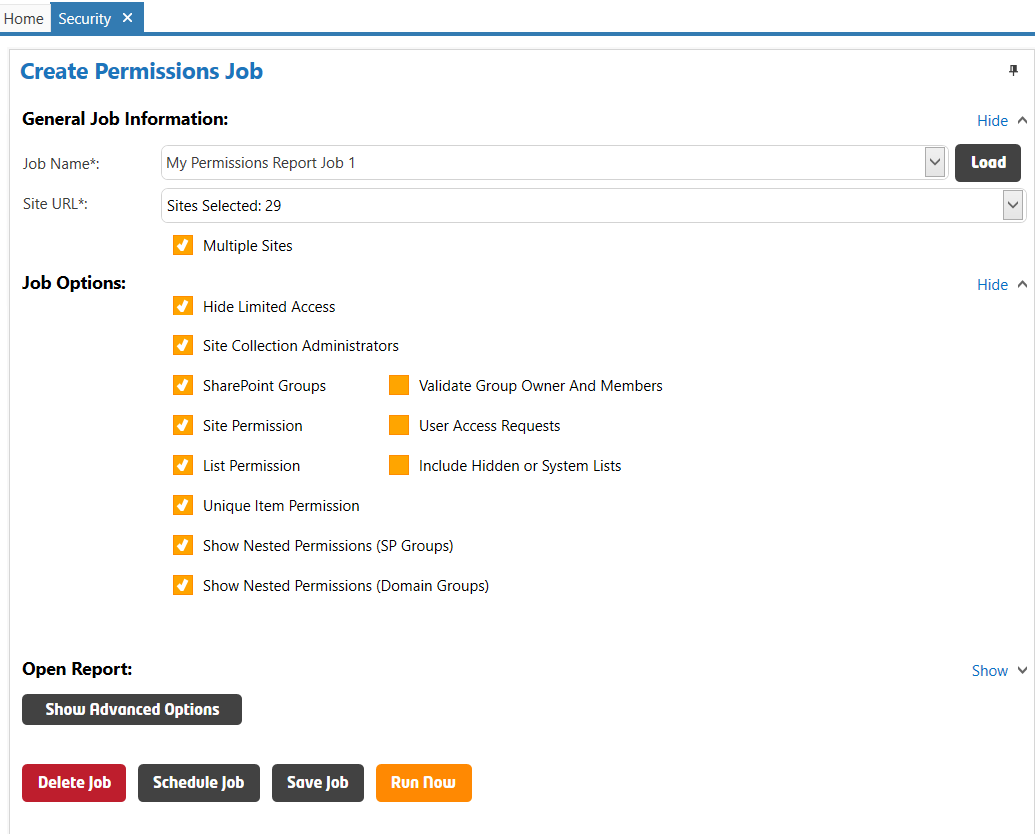


1. You can minimize the tool and the job will continue to run. Once complete, you will be notified:  
     
     
   
2. Select one of the report buttons/links to open one of the Permission reports:



## Report Options

This section will provide details of each option found when generating Permission Reports



\*Denotes a required field

### 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

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 the Home Page Dashboard by right clicking on one or more sites.

### **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>

**Details:** When a user is assigned permission for an object (meaning a SharePoint list/library, folder, item, file, web page), but not the parent (such as at SharePoint site level), the parent object will show “Limited Access” since the user has permission to a child object but not parent.  
Example: John has permission to view a file in Documents library, but does not have access to everything in the Documents library, John will show as having “Limited Access” in the report (and in SharePoint) at the library and site level, since John has access only to one or more child objects but not at the library or site level.

### **Site Collection Administrators**

Select this option to build a report on the Site Collection Administrators for all selected site collections.

### SharePoint Groups

Select this option to include a list of all SharePoint Groups for the selected Site Collections. This report will show SharePoint Group settings, the SharePoint Group Owner, members of each group.

TIP: You can add or remove Owners, and SharePoint Group Members in bulk from within the generated report within the tool.

#### Validate Group Owner and Members

Use this option to validate all SharePoint Group Owners and Members to determine if the account exists and is enabled in Active Directory/Azure AD. A column labelled ‘Status’ will indicate if the account is present and valid/active.

### **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.

#### User Access Requests

Select this option to include all User Access Requests for the selected sites. A User Access Request occurs when a user is prompted that the SharePoint site, page, file, item or list is not accessible, the user can click to “Request Access”. These access requests and the invitation status is shown in the report.

TIP: You can Accept or Reject invitations (in bulk) directly from within the report using the tool.

### **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.

#### **Include Hidden or 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.

### **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.

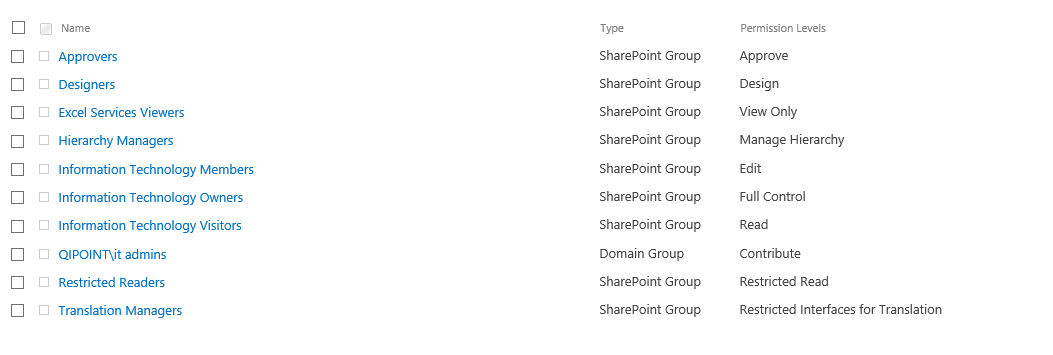
If this option is turned on (checked), the tool will also display all permissions, such as AD Users and AD Groups, nested within all SharePoint Groups found.

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 inside 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 (Domain Groups)**

Select this option to display user permissions nested within Active Directory (AD) Groups/Azure Active Directory (AAD).

NOTE: If your organization has several large AD Groups (over 10K AD members in any one or more AD groups), you can set AD Groups to exclude in the Exclusion Rules.

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 (Domain Groups)’ is disabled, only these objects below will show in the report. If ‘Show Nested Permissions (Domain 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 “COGNILLO\it admins” (labelled with Type = “Domain Group”). With the option “Show Nested Permissions (Domain 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.

### Open Report

**Open Report Site Permissions** – Select “I’ll Open Report Myself” or “Automatically Open Once Job Completes” drop-down choice to manually or automatically launch the Site Permissions report when the job completes.

**Open Report List Permissions** – Select “I’ll Open Report Myself” or “Automatically Open Once Job Completes” drop-down choice to manually or automatically launch the List Permissions report when the job completes.

**Open Report Unique Item Permissions** – Select “I’ll Open Report Myself” or “Automatically Open Once Job Completes” drop-down choice to manually or automatically launch the Item Permissions report when the job completes.

**Open Report Site Collection Administrator** – Select “I’ll Open Report Myself” or “Automatically Open Once Job Completes” drop-down choice to manually or automatically launch the Site Collection Administrator report when the job completes.

### Credentials

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

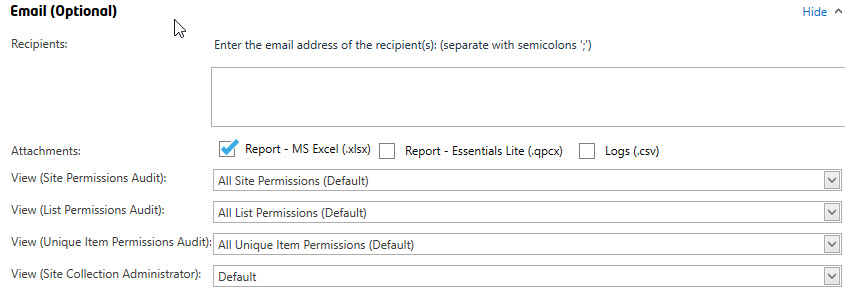
**Default SharePoint Authentication** – Automatically determines Authentication to connect to the SharePoint site. This will work in most cases when SharePoint is hosted on your internal company network. Enter the custom credentials to use for this site. If your environment uses a custom login screen,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

### Email (Optional)



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 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.

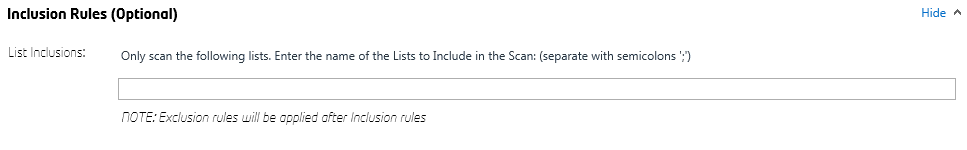
*Report – Essentials Lite (.qpcx)*   
Optionally include a Cognillo Essentials Lite report as an attachment. The client must have the Cognillo Essentials Lite Client (ClickOnce application) installed on their computer to open this type of report.

*Logs (.csv)*   
Optionally include the log files as a compressed/zipped, email attachment.

**View** – (Only applies to MS Excel Report, not SharePoint List Exports or Cognillo 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).

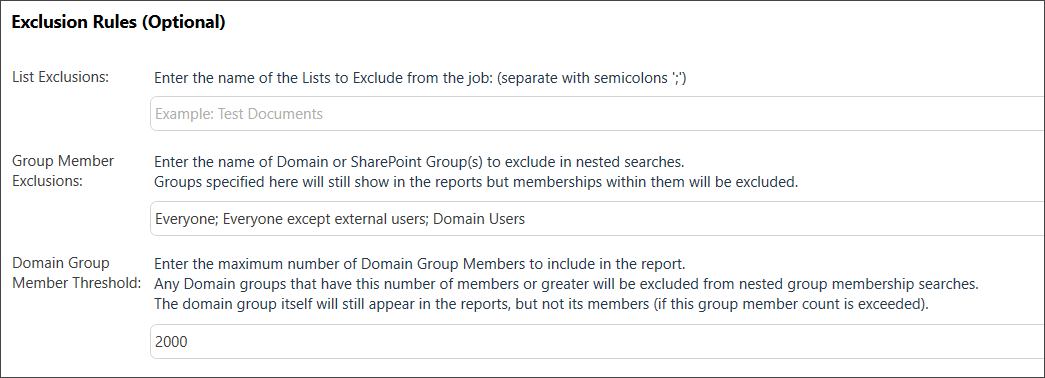
You can select a custom view from the drop-down list to apply it to the MS Excel file that is emailed to the user(s). All grouping, sorting and filtering set in these views will be applied to the MS Excel report. If you use the default view, MS Excel will show a flat list without any grouping or filtering.

### 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

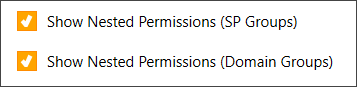


#### List Exclusions

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.

#### Group Member Exclusions

This option is only applicable if one or both of the “Show Nested Permissions” are selected.

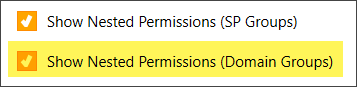


Enter the Domain or SharePoint Group you want to exclude in the nested search, using the “Show Nested Permissions (Domain Groups)” checkbox, located in the above Report Options section.

Groups specified will display in the reports, however, the nested membership (users within those groups) will not show in reports. Specify multiple Domains or SharePoint Groups here, separated by semi-colons.

#### Domain Group Member Threshold

This exclusion is only valid if “Show Nested Permissions (Domain Groups)” option is selected.



The default value is 2000. This represents the maximum number of members inside of an Active Directory Domain Group to include in the report. Domain Groups with a greater number of members than this value (such as 2001 members in the group), will not be parsed for the members and the members will not be displayed in the report.

This is useful for organizations who may want to display users who have access via Domain Groups, however have many large domain groups where they do not want to include in the reports.

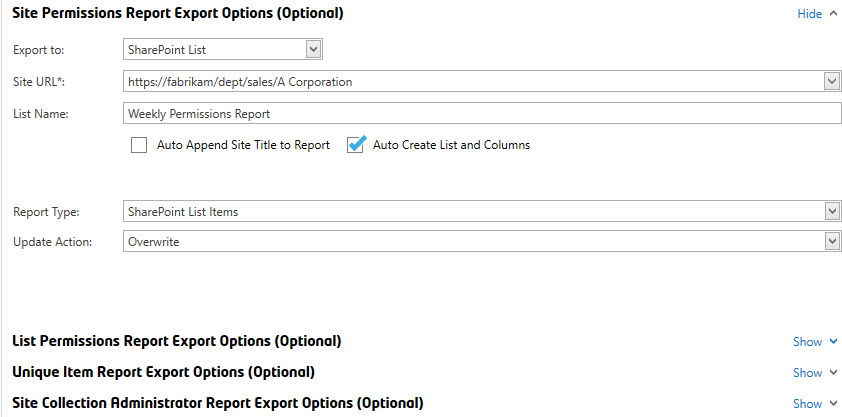
This value compares against the members directly within the AD Group, it does not count nested AD Groups within AD Groups.

### Report 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*

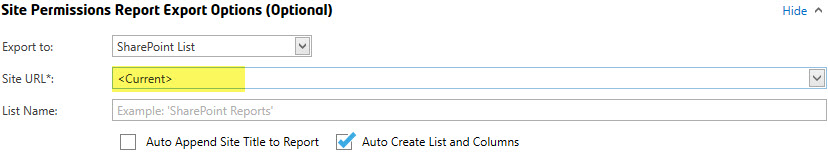


**Note**: The ‘MS Excel / CSV’ and ‘SharePoint List’ export options are also available for the List Permissions Report Export, Unique Item Report Export, as well as the Site Collection Administrator Report sections.

**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 from Home Page Dashboard by check-marking several sites. 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 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”

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.

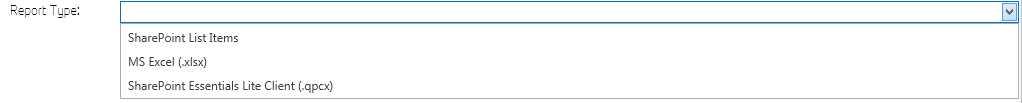
**Report Type**

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



If this job targets bulk sites (when creating reports against multiple site collections) checkmark sites from the 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 append 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 a 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. 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.

**Auto Append Site Title to File Name**

Available for the Report Type ‘MS Excel (.xlsx)’ and SharePoint Essentials Lite Client (.qpcx).

**View**

The drop-down menu is available for the Report Type ‘MS Excel (.xlsx)’ and displays the “All Links (Default)” choice/option.

### Discover (section in Left Navigation)

This Left Navigation also allows you to generate new Permissions Reports. This is equivalent to Method 2 above and selecting ‘New Report’.

#### New Job

This will create a new Permissions report for one or more **SharePoint Sites** It will generate a ‘Comprehensive Report’, a Site-level, List-level and Item-level permissions report.

#### Check User Permissions

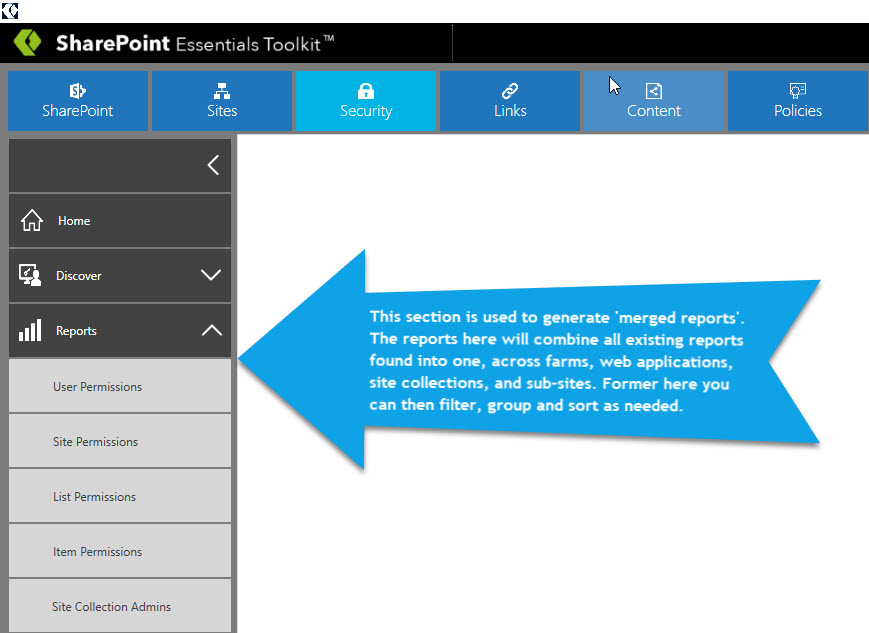
This will create a new Permissions report for a given **User or Group**. You will be prompted to select the user to report against. It will generate a single report that includes all permissions for the user granted at the Site-level, List-level and Item-level. See “[Check User Permissions Reports](#_Check_User_Permissions)” 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.

### Reports (section in Left Navigation)

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 (most recent) 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.

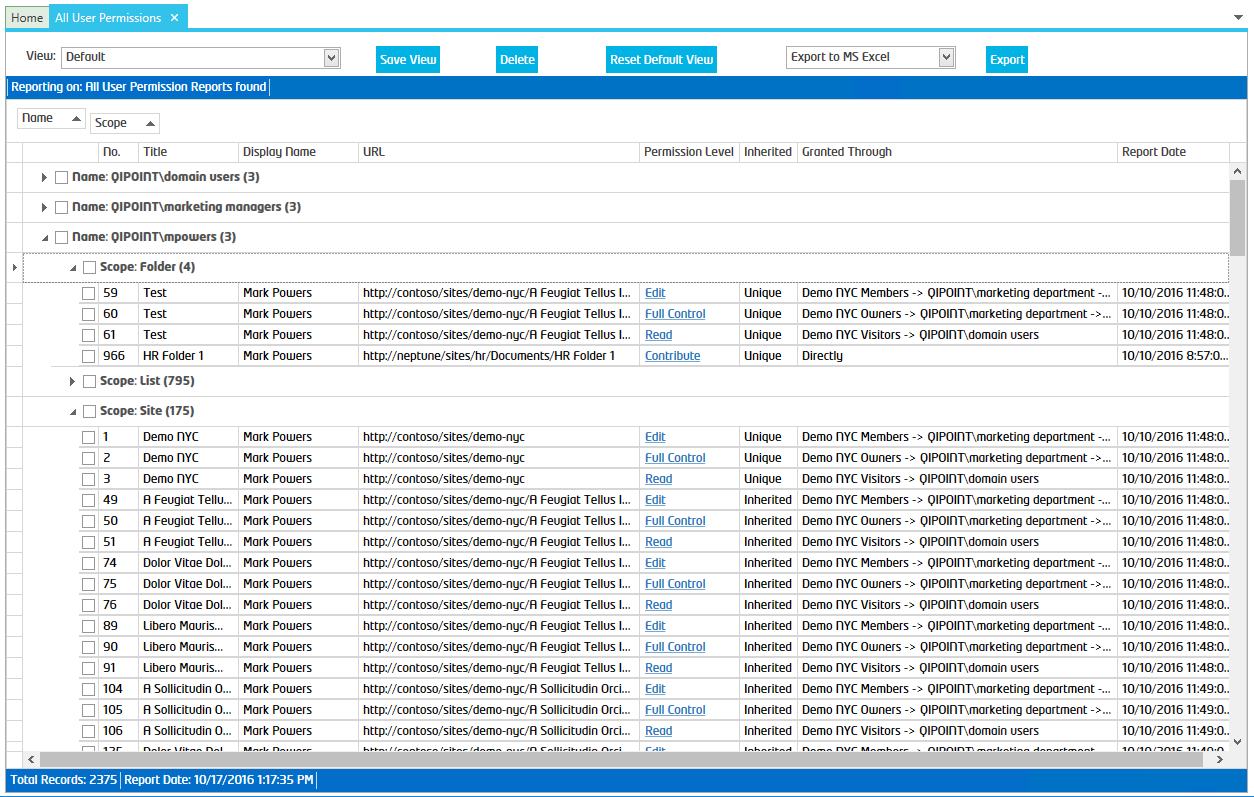


#### User Permissions

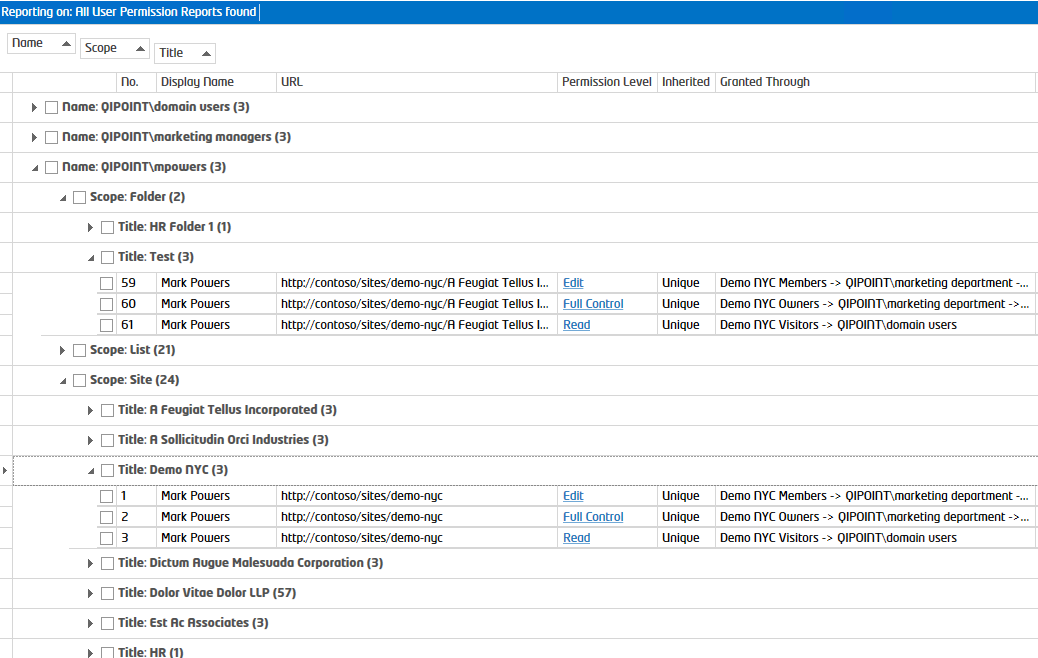
This will create a merged Check User Permissions report. This will display all permissions for the Users that you have “Checked Permissions” for. This requires at least one “Check User Permissions” report to have been generated.

For example, you can run a job on a schedule for specific accounts in your organization, then use this report to view the permissions granted for each of member and where they have access for the sites you manage.

Example Below:



Another View of the same report:



#### 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 Site Permissions Report.

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 those sites using this single ‘merged’ report.

#### List Permissions

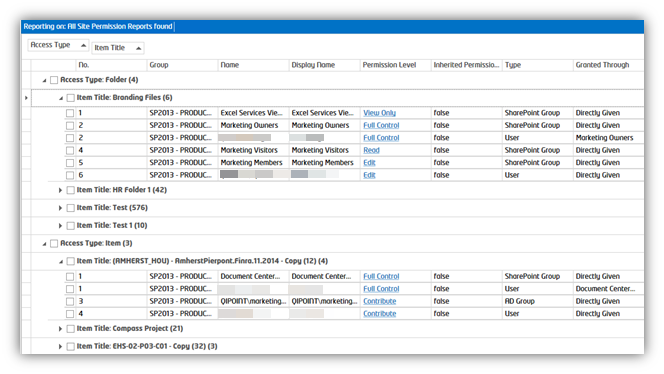
This will create a merged Check User Permissions report. This will display all List Level permissions for all SharePoint Sites that you have List Permissions Report.

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

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



#### Site Collections Admins

This will create a merged Site Collections Admins permissions’ report. This will display all Admin Level permissions for SharePoint Sites that you have created a Site Collections Admins permissions’ report.

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 those sites using this single ‘merged’ report.

## Check User Permissions Reports

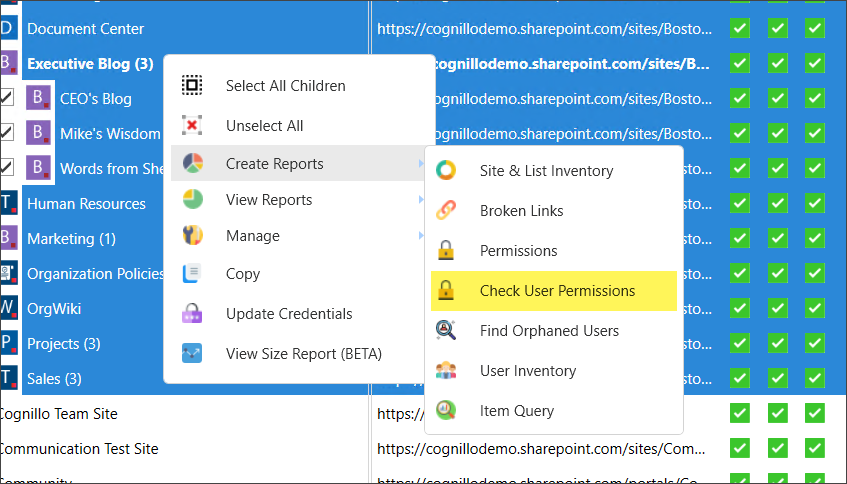
This report is used to identify all content that a user, Active Directory (AD) group, or SharePoint Group has access to. If you are checking a user’s access, this report will show access granted via SharePoint Group or direct access (where the user was added directly to the site/list/item). You can also optionally “Include Domain Group Membership” to check the user’s access, that has been granted through an AD Group in SharePoint.

**NOTE**: 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.

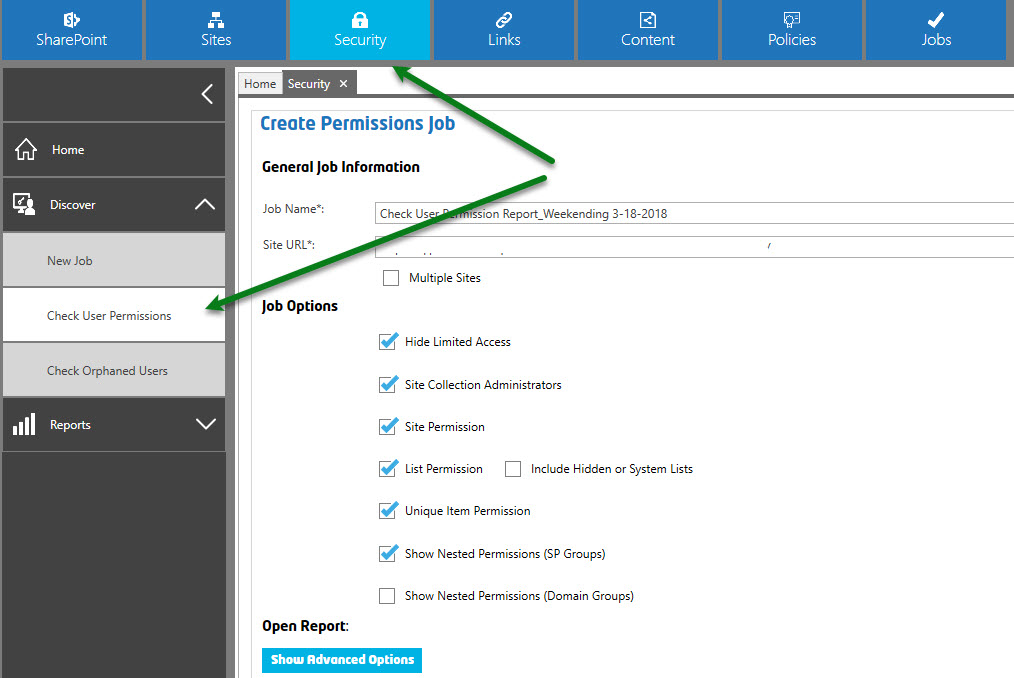
### How to Create a User Permissions Report

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

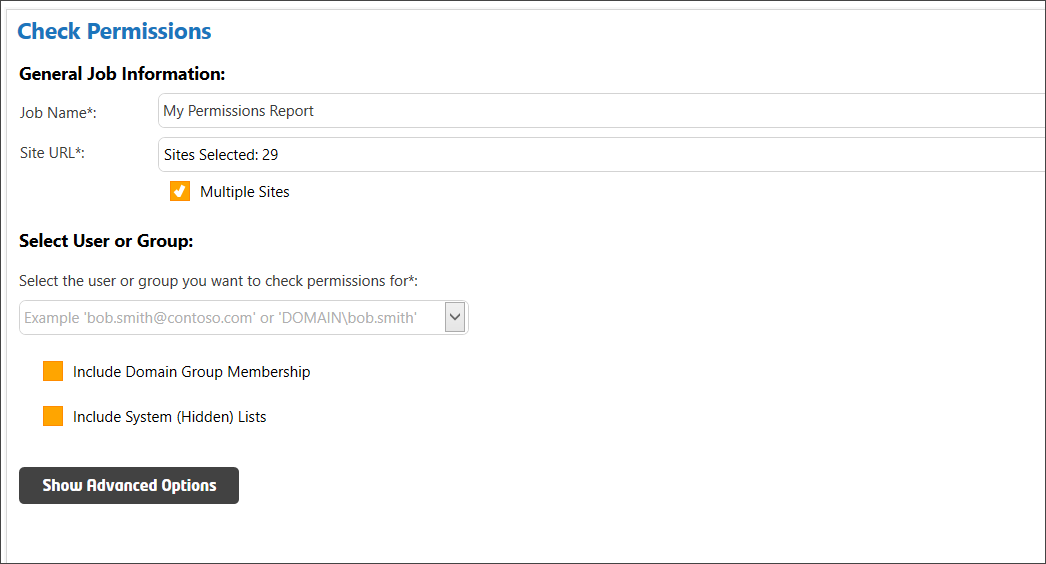
1. From the Home Page Dashboard, select one or more sites. Then right click and click ‘Create Reports->Check User Permissions’.

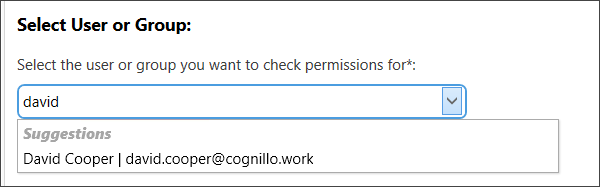
Below I chose to check a user’s permissions across multiple sites in multiple site collections:  


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. In the “Select Users or Group” section, enter the display name/email or account name of the user/group who you want to check permissions for. After typing at least three (3) valid characters, the tool will show suggestions based on your input. You may see multiple display names if multiple accounts are found, depending on the previously typed characters.  
   

TIP: If no results are shown, be sure to select/enter the Site URL before typing the user name.

1. Click on the “Show Advanced Options” button, and then enter the “Credentials” of the ‘User Name’ and ‘Password’ to connect to the previously specified ‘Site URL’.
2. Click the “Run Now” button to create the report. If multiple sites are selected, it will iterate all sites and build a single report.

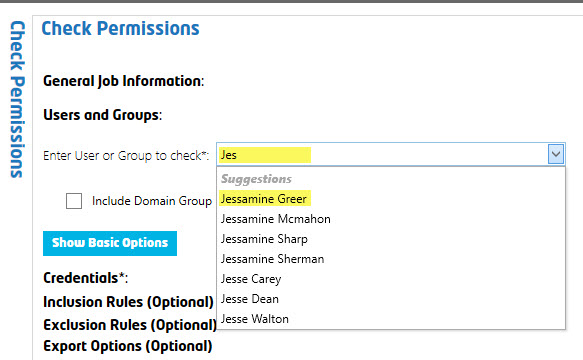
#### General Job Information

##### 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.

#### **Users and Groups**

Enter the Active Directory (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 Domain Group Membership** – 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.

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

##### Credentials

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

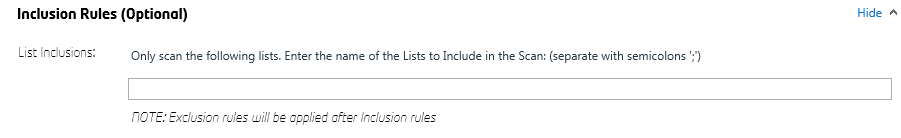
**Default SharePoint Authentication** – Automatically determines the authentication to connect to the SharePoint site. This works in most cases when SharePoint is hosted on your company’s internal network. Enter the custom credentials to use for this site. If your environment is using a custom login screen, such as one that requires Multi-Factor Authentication/a PIN, ADFS or has SSO enabled, use the 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, ADFS or has SSO enabled, use this authentication type. If you want to schedule jobs, click the “Remember Credentials” checkbox and run the job once; the system will remember these credentials for a schedule job.

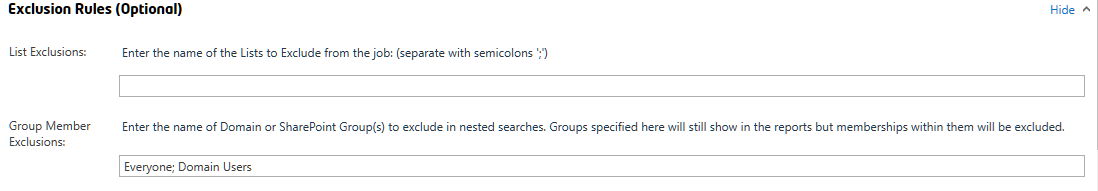
**Remember Credentials -** Select this option to store the username and password. Passwords are stored using strong ‘salted’ encryption.

### Inclusion Rules (Optional)



**List Inclusions** - Use this section to filter and only scan specific SharePoint Lists in the job. Use the *List Title* (display name), not the List URL here. The user can specify what list(s) to include in the report by entering the name of the list in the textbox. 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. 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 the word ‘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 each list name with a semi-colon ‘;’.

### Exclusion Rules (Optional)



**List Exclusions** - 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 list(s) to exclude in the report by entering the name of the list in the textbox. If the name of the list exists in multiple sites, they will all be excluded if the *List Title* (display name) matches. Wildcards (\*) are supported. 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 the word ‘documents’ will be excluded in the scan.

**Group Member Exclusions -** The user can enter Groups to exclude if parsing their members. This is useful when you have groups with many members, such as ‘Domain Users’ or ‘Everyone’, which would cause the program to take a long time to return all members/results in some cases.

In this field, the user can enter group (display name) names to exclude from the job. Groups entered here will still be visible in the job, however, the memberships within these groups will not be enumerated (such as User members would not show up in the reports).

### NOTE: Inclusion/Exclusion Rules:

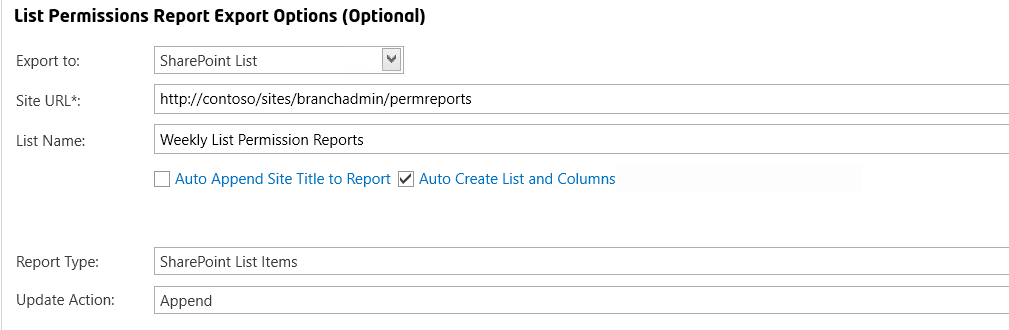
* **Exclusion rules are applied AFTER Inclusion rules (if any).**

### Export Options (Optional)



This section 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.

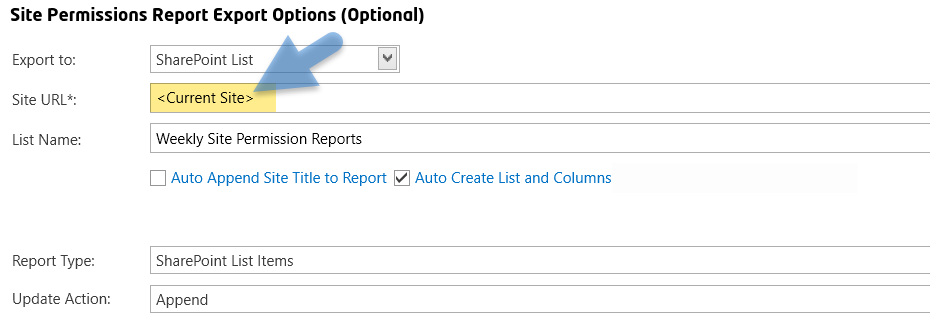
#### Export to: SharePoint List



**Site URL**

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

<Current Site> - You can use this token / keyword (as shown below) to use the currently scanned site. If you have performed a ‘multi-threaded’ job by check-marking several sites from the Home Page Dashboard, the report will export to the current site being scanned.



**List Name**

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

**Auto Append Site Title to Report**

Check this option to 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 generated SharePoint List report will show as “Weekly User Permissions Report - Information Technology”.

**Auto Create List and Columns**

Check this option to automatically attempt to create the List and Columns (this option is checked by default). 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.

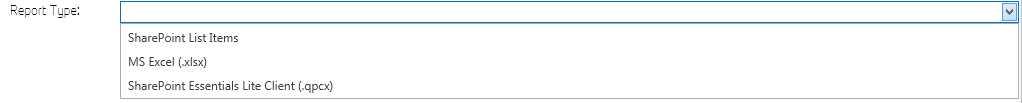
**Report Type**

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 Domain Group Membership” and have over 5,000 account memberships within one or more Active Directory Groups), this option may make the list a “Large List” of over 5,000 items. If you have many permission objects and do not want to reach this threshold, please use one of the other file options below):

1. MS Excel (.xlsx) – The report will upload as a MS Excel (.xlsx) file.
2. SharePoint Essentials Lite Client (.qpcx) – The report will upload as a .qpcx file. This file type can be opened an end user who installs our free SharePoint Essentials Lite Client (WPF ClickOnce application).



**NOTE:** If this job targets bulk sites (when creating reports against multiple site collections) checkmark sites from the 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 append 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 a single report (a single SharePoint List).

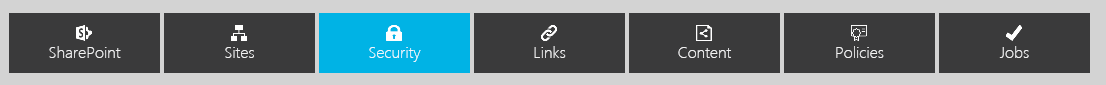
**Update Action**

Overwrite: This choice 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 the list’s settings and views remain intact.

Append: This choice will append the 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 the QPCX format, this option will append the new report by adding a date and 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, as well as have the old versions drop off based on the library major versions limit.

Update: (Available for SharePoint List Item Export) This choice 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 reported site.

## Check Orphaned Users



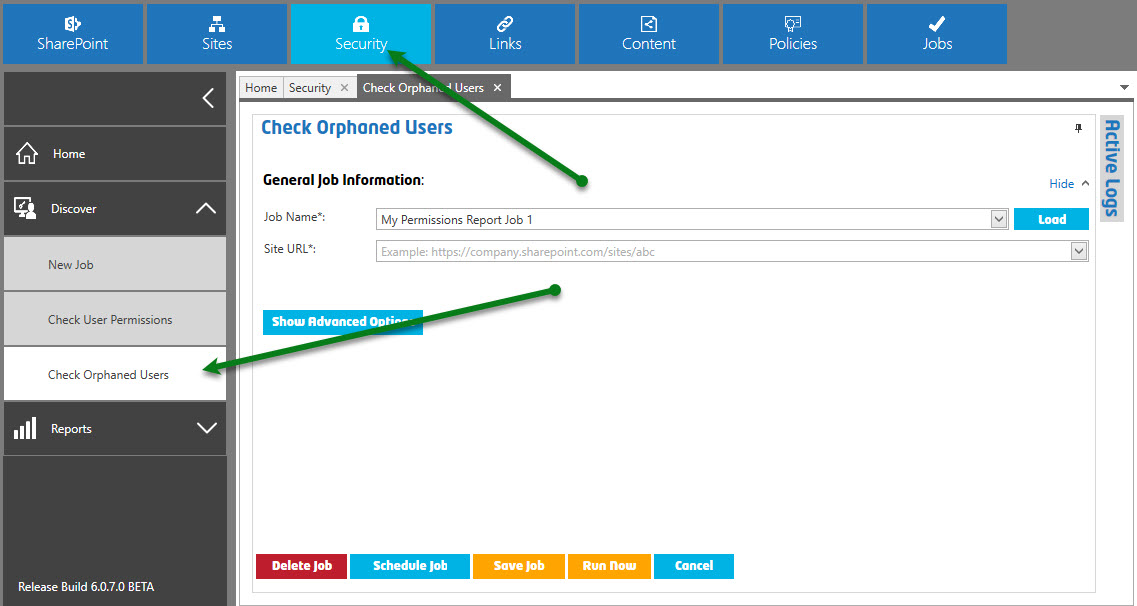
This creates a report that shows all orphaned users. An “Orphaned User” is a user object in SharePoint that does not have a corresponding Active Directory (AD) Account. This could be a disabled or deleted AD user or group account.

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

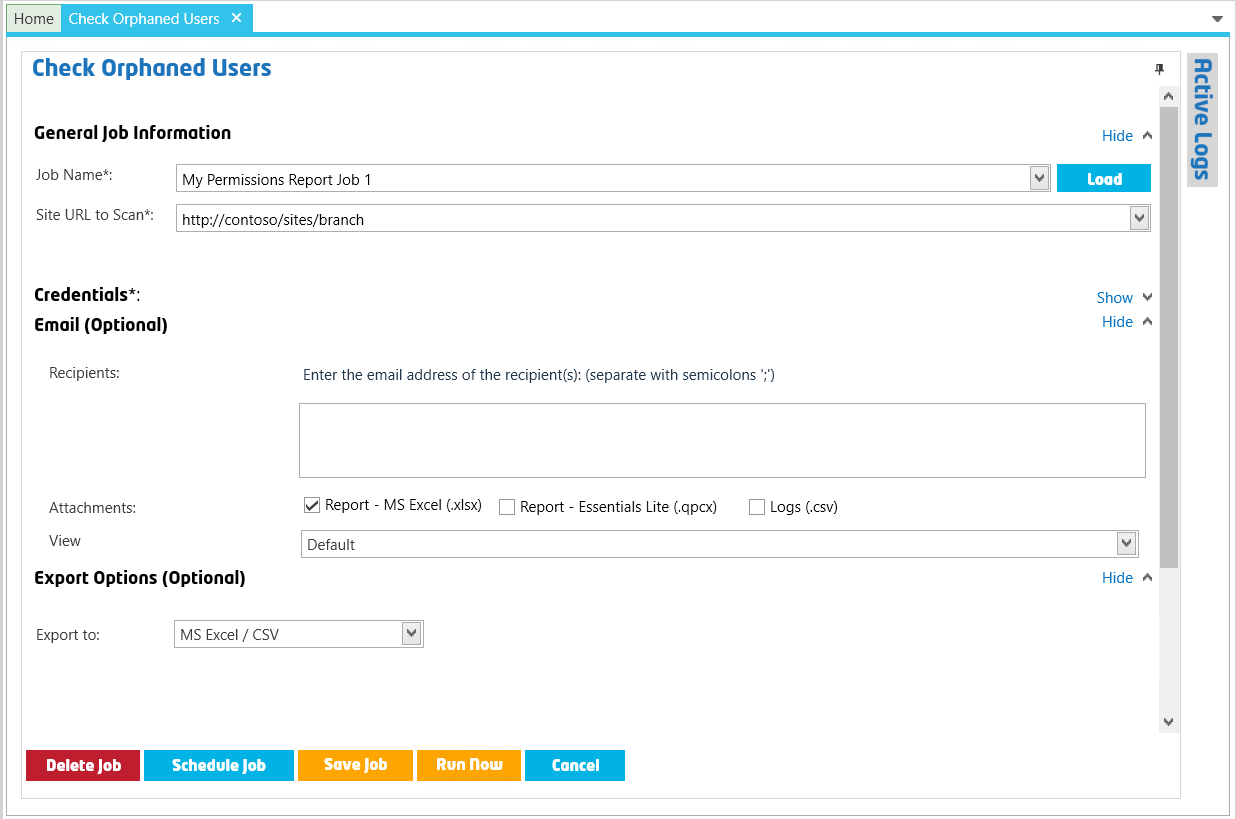
### How to Create an Orphaned Users Report

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, and then click the “Check Orphaned Users” option.



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



1. You can enter a Job Name or leave the default text.
2. Enter or select the site to check in ‘Site URL to Scan’ drop-down menu.
3. Enter any other options here (if applicable). More details are available below.
4. Click the “Run Now” button to create the report.

#### General Job Information

##### 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

This is the absolute URL of the site you want to scan to generate 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/>

**Note**: Do not include the page path in the URL.

### Show Advanced Options

##### Credentials

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

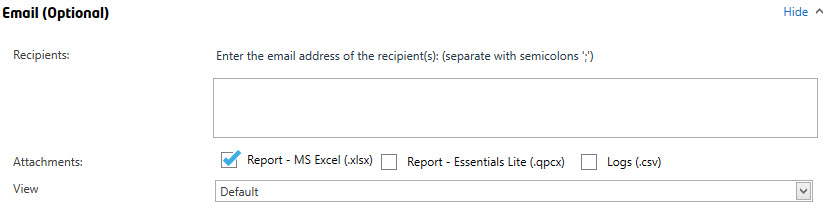
**Default SharePoint Authentication** – Uses Windows Authentication to connect to the SharePoint site. This will work in most cases when SharePoint is hosted on your internal company network. Enter the custom credentials to use for the site. If your environment uses a custom login screen, such as one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

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

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

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

##### Email (Optional)



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

*Logs (.csv)*   
Optionally include the log files as a compressed/zipped, email attachment.

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

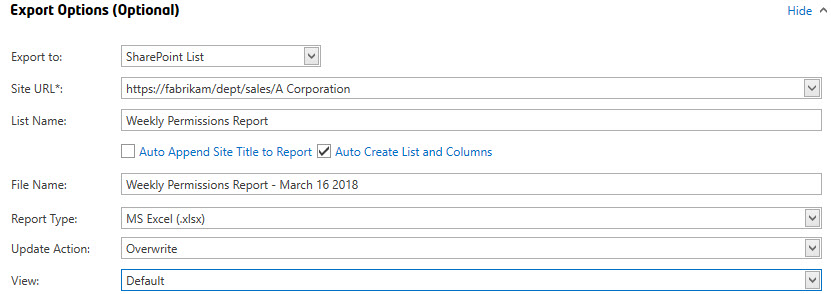
You can select a custom view from the drop-down list to apply it to the MS Excel (.xlsx) file that is emailed to the user(s). All grouping, sorting and filtering set in these views will be applied to the MS Excel report. If you use the default view, the MS Excel report will show a flat list without any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

##### Export Options (Optional)



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

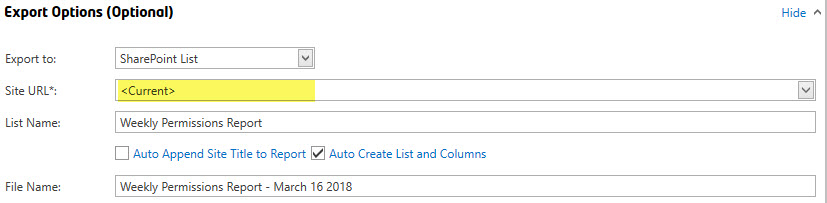


**Note**: The ‘MS Excel / CSV’ and ‘SharePoint List’ export options are also available for the List Permissions Report Export, Unique Item Report Export, as well as the Site Collection Administrator Report sections.

**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 from Home Page Dashboard by check-marking several sites. 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.

**File Name**

This is the name of the file *to b*e given to report for the Report Type ‘MS Excel (.xlsx)’.

**Note**: The File Name field is not applicable to the Report Type ‘SharePoint List Items’ only.

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”

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.

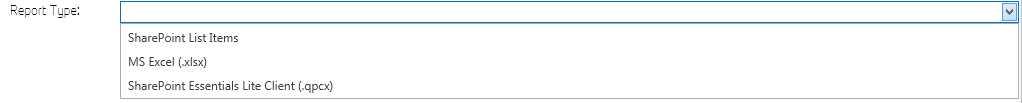
**Report Type**

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 (Domain Groups)” and have 10K+ users in an Active Directory Group, this option may make the list a “Large List” of over 5,000 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 (.xlsx) file – The report will be uploaded as a MS Excel File.
2. SharePoint Essentials Lite Client (.qpcx) – The report is uploaded as a .qpcx file. This file type can be opened by any end user who installs our free SharePoint Essentials Lite Client (WPF ClickOnce application).



If this job targets bulk sites (when creating reports against multiple site collections) checkmark sites from the 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 append 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 a 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. 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.

**Auto Append Site Title to File Name**

Available for the Report Type ‘MS Excel (.xlsx)’ and SharePoint Essentials Lite Client (.qpcx).

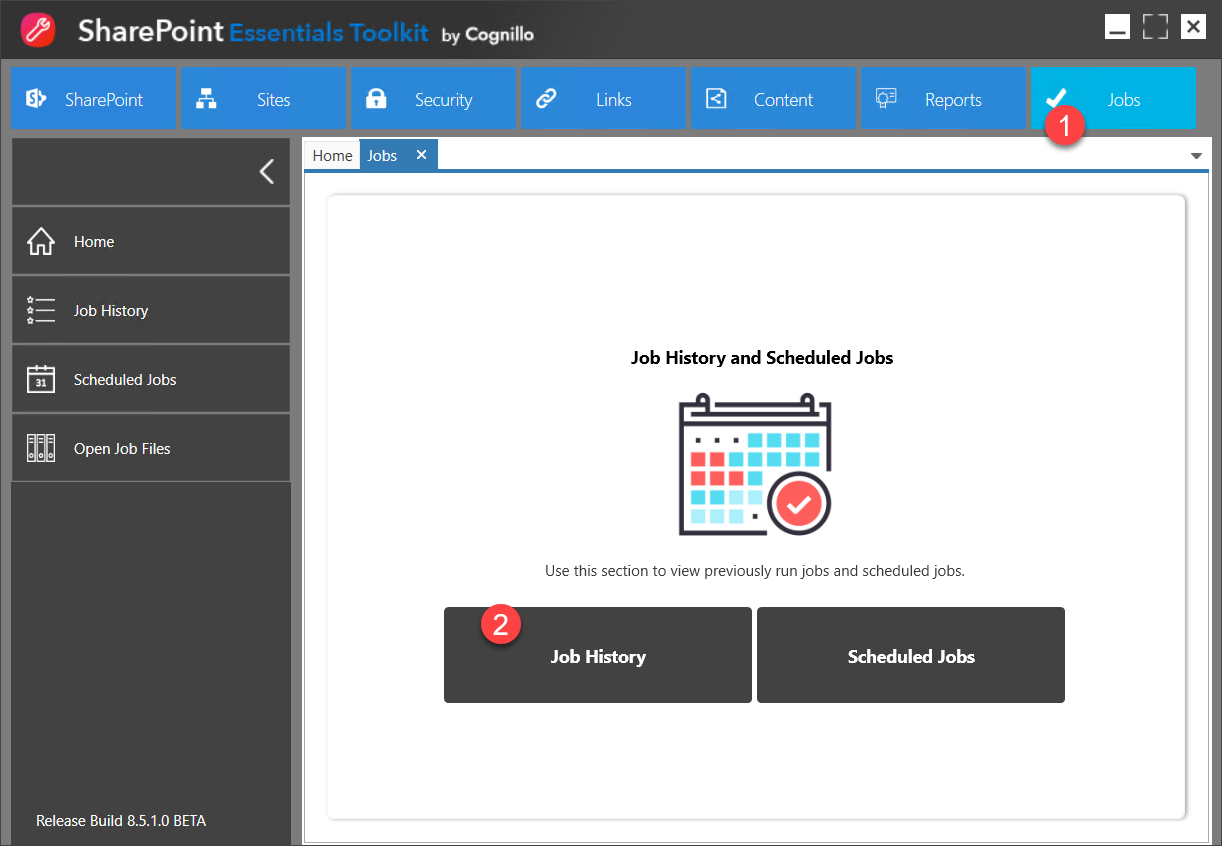
**View**

The drop-down menu is available for the Report Type ‘MS Excel (.xlsx)’ and displays the “All Links (Default)” choice/option.

## Logs

While a Job runs, logs are generated in real-time, allowing the user to view the status and progress of the job.

You can view Job Logs by going to Jobs->Job History

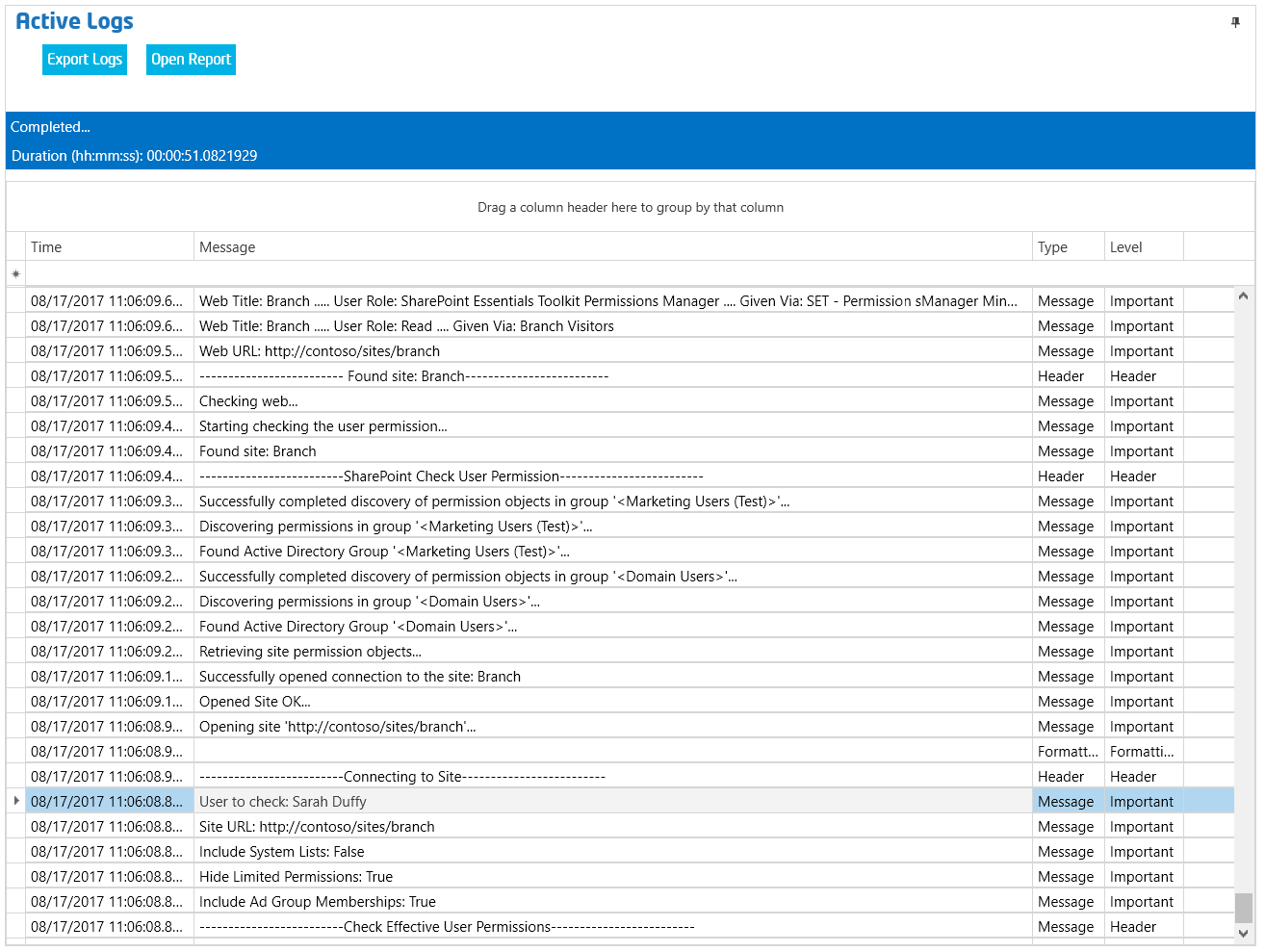


### Physical Log files and reports

These are stored under the Settings page (Home -> Settings -> Path to Store Reports) in the SharePoint Essentials Toolkit.

Normally you can view any log by navigating to the Home Page Dashboard, right clicking on the site you ran the job for, and then clicking on “View Logs”. You can also view logs from the top navigation tile: Job -> Job History page. If the job was scheduled, the logs are also accessible through the path: Jobs -> Scheduled Jobs window.

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



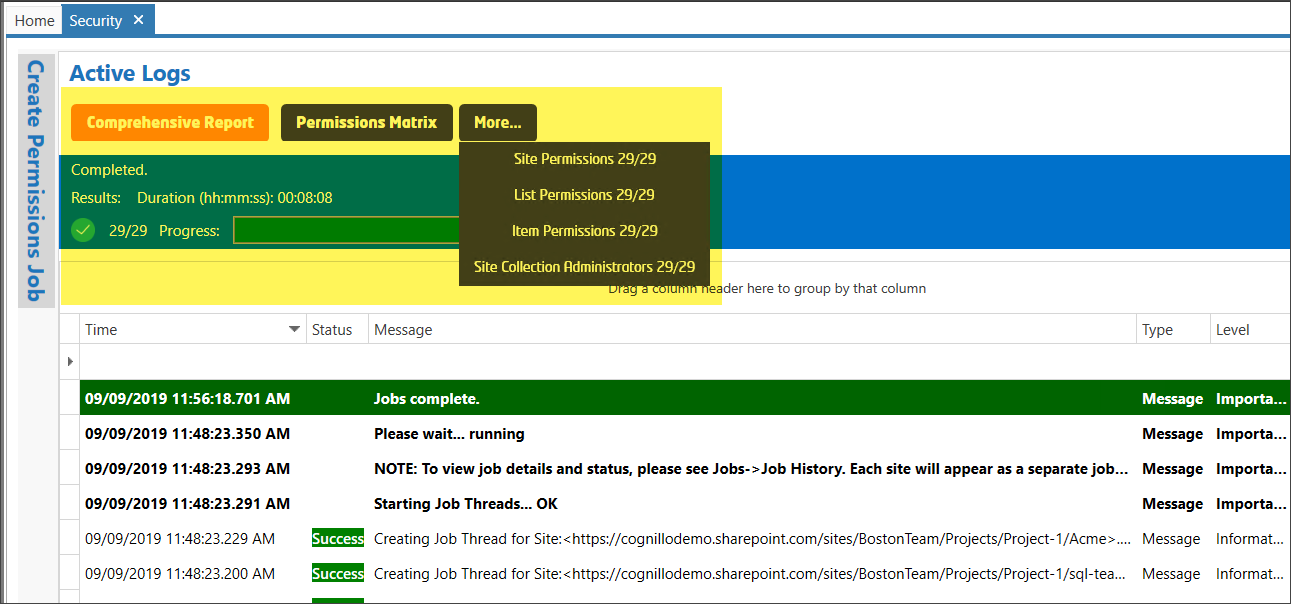
### Export Logs

You can export job logs to CSV format by clicking the “Export” button when viewing a job’s log.

## Opening Reports / Viewing Historical Reports

### Open report for current Job

You can open a report after a job is completed by clicking on one of the report buttons:

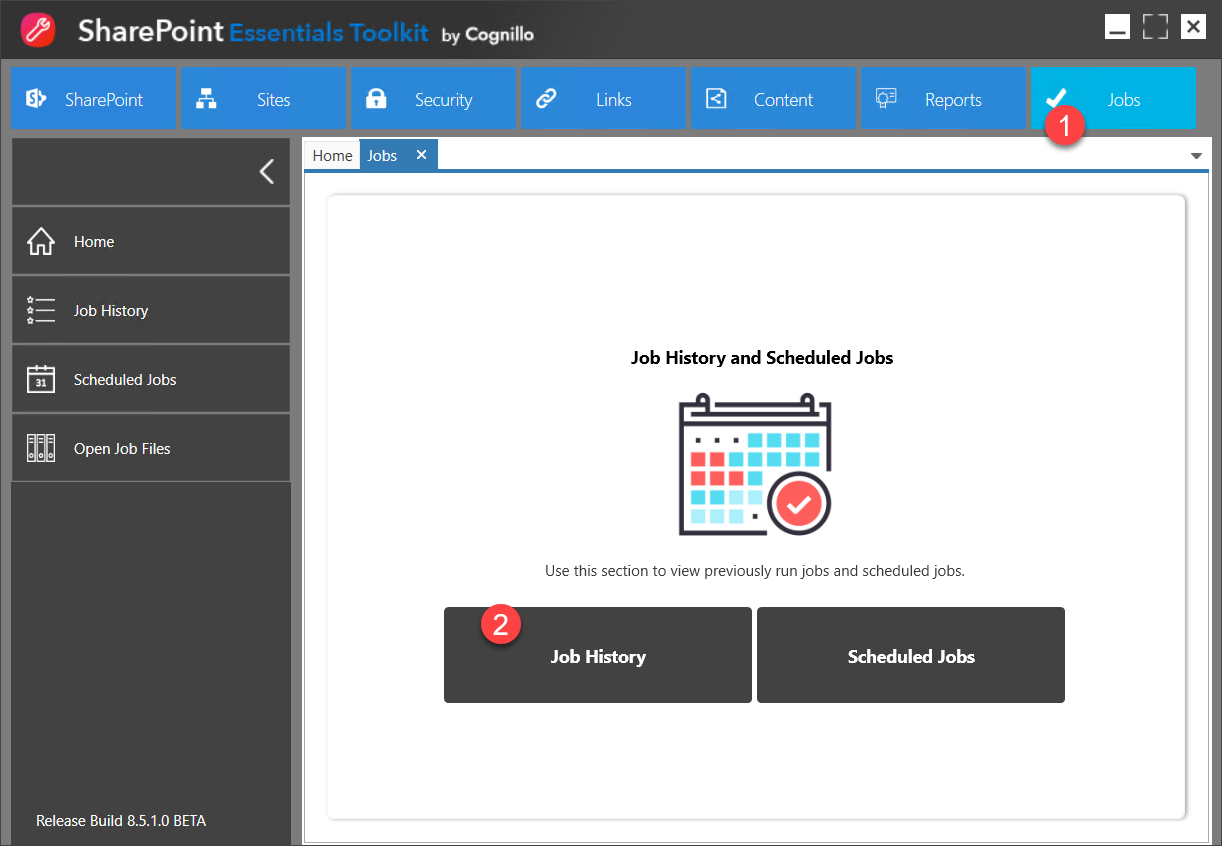


### Past Jobs / Historical reports

For past jobs, you can find these in one of two places: Job History, or the Home Page Dashboard

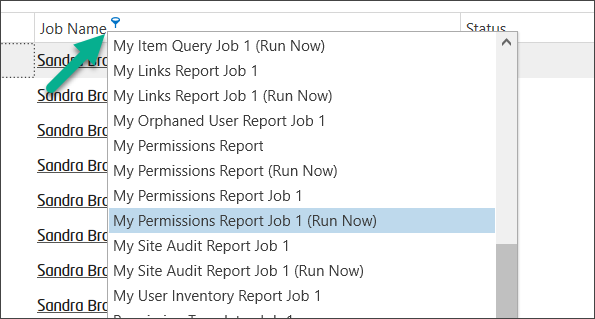
#### Job History

Go to Jobs->Job History:

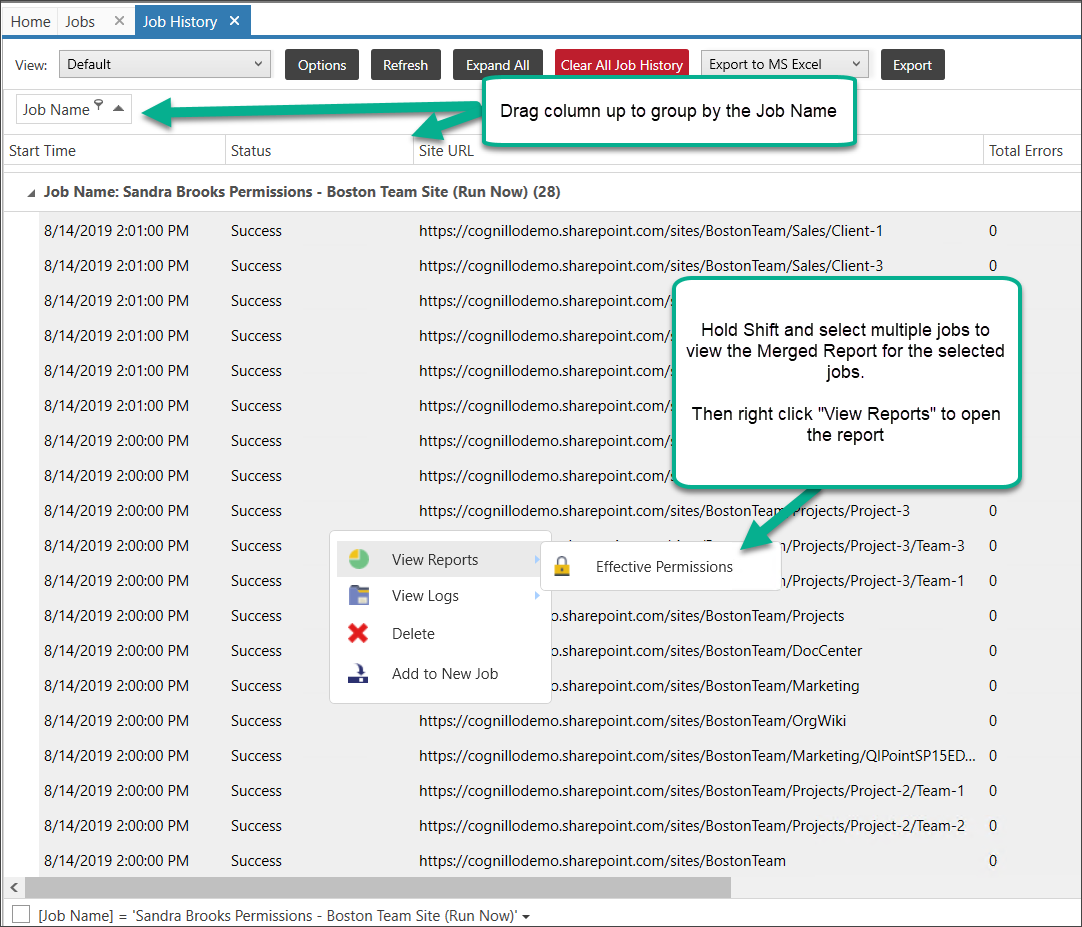


Then select the Job(s) to include in the report you want to view.

You can filter by Job Name:



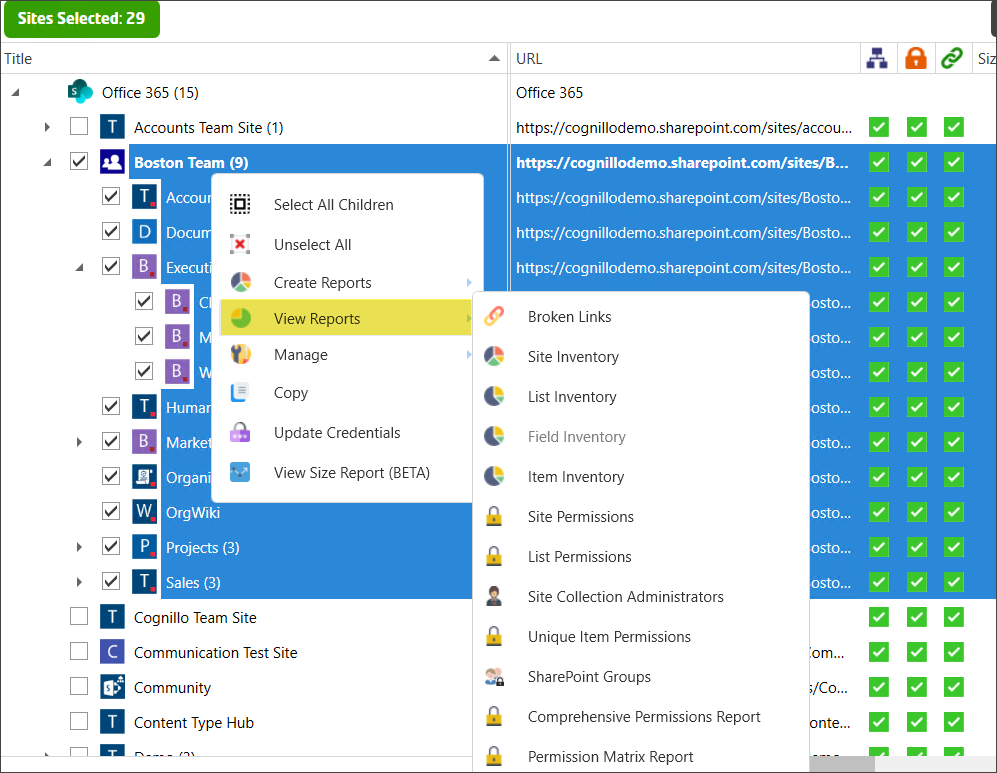
You can drag by Job Name to group all reports for a specified job:



Hold Shift and select multiple jobs to view the Merged Report for the selected jobs. Then right click "View Reports" to open the report

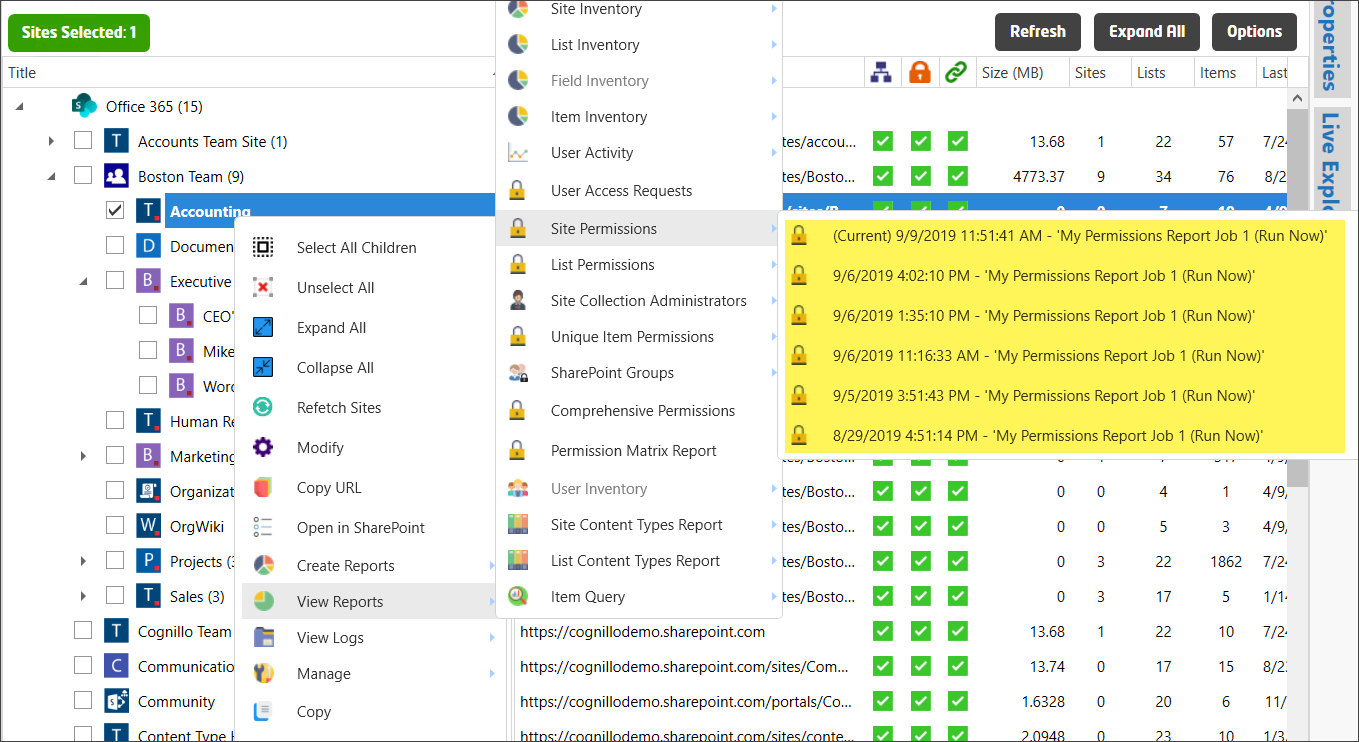
#### Home Page Dashboard

Select one or more sites from the Home Page Dashboard. Right click and select “View Reports”



This will open a merged report for the selected sites of the most recent job run for them.

If you select a single site, you can view up to 5 past jobs. If you need previous jobs, use the Job History section (above)

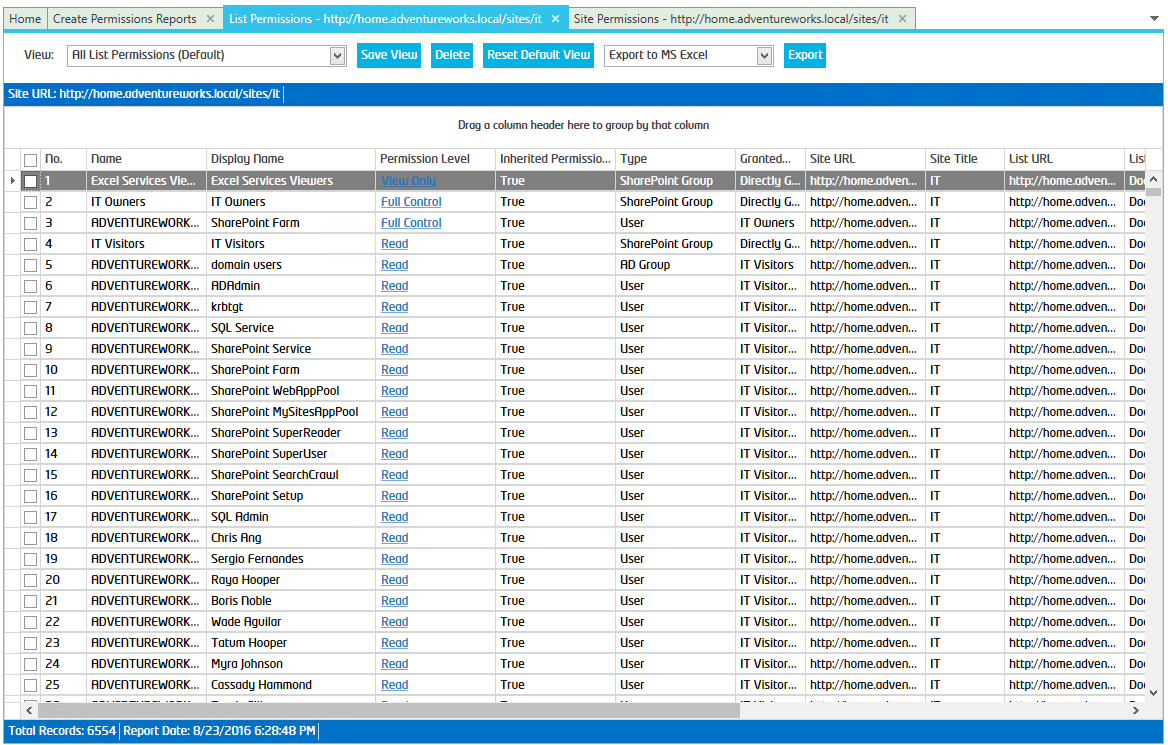


# How to Interpret the Reports

## 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, followed by sorting, and then applying advanced or simple filtering to generate a useful report to align with 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

#### Permissions Reports

There are 8 types of Permissions Reports:

1. Comprehensive Permissions Report
2. User or Group Permissions
3. Site Permissions
4. List Permissions
5. Item Permissions
6. Site Collection Administrators
7. SharePoint Groups
8. User Inventory

These are shown below.

Once a job is complete, you can open a Permissions Report in several ways:

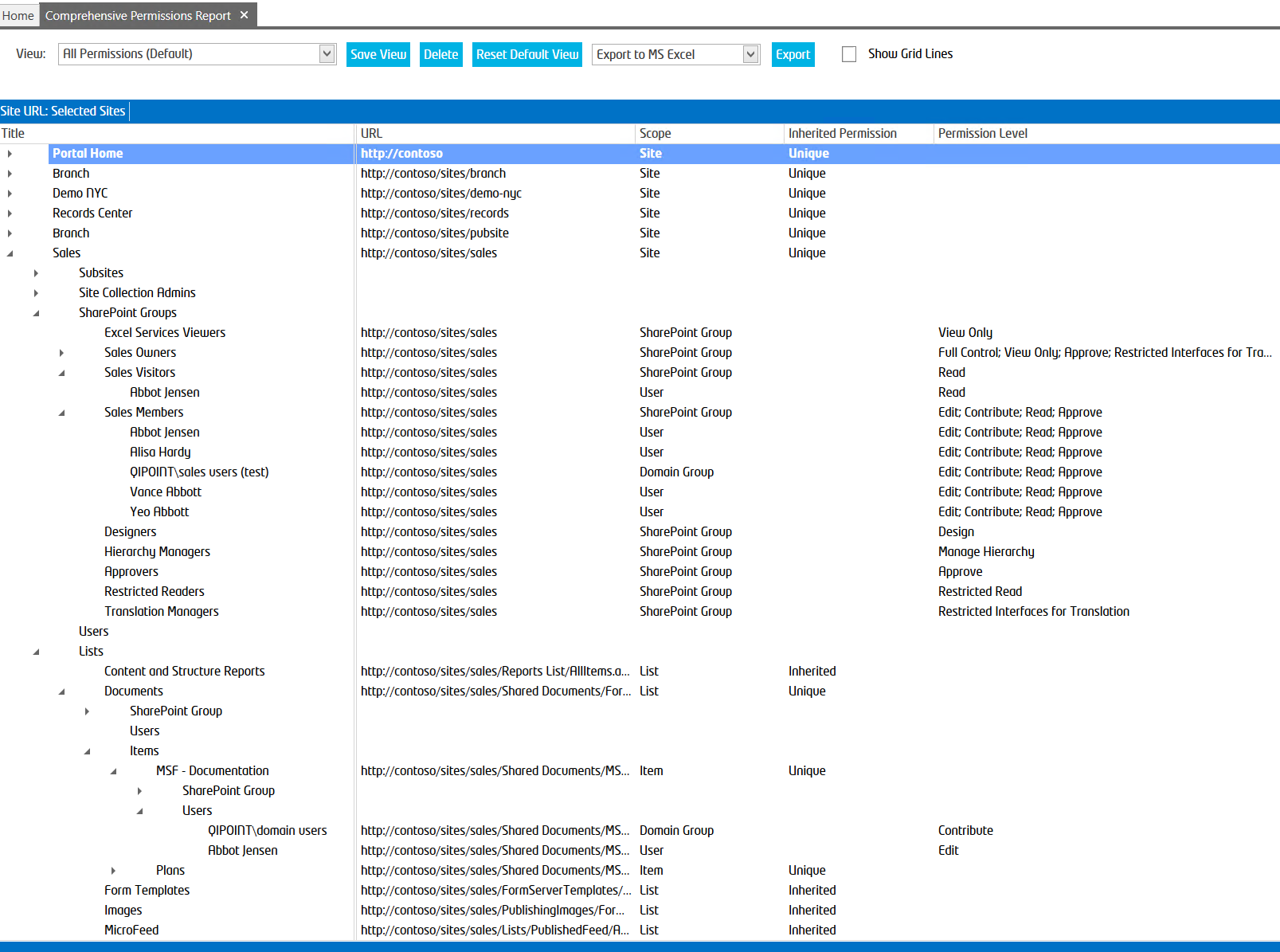
* + On the top-left (below the “Active Log” window name) that says, “Open Report”.
  + Once you click “Open Report” and the report opens, you can click the “Export” to view the report in Excel/CSV/SharePoint/QPCX format.
  + From the Home Page Dashboard, you can right click on a site that you wish to preview, and then click the “View Reports -> Permissions Report”.
  + From the “Job -> Job History” page you can find previously created jobs, along with 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 “Cognillo\Reports”. You can change the report path under “Home -> Settings -> Path to Store Reports”

#### Comprehensive Reports

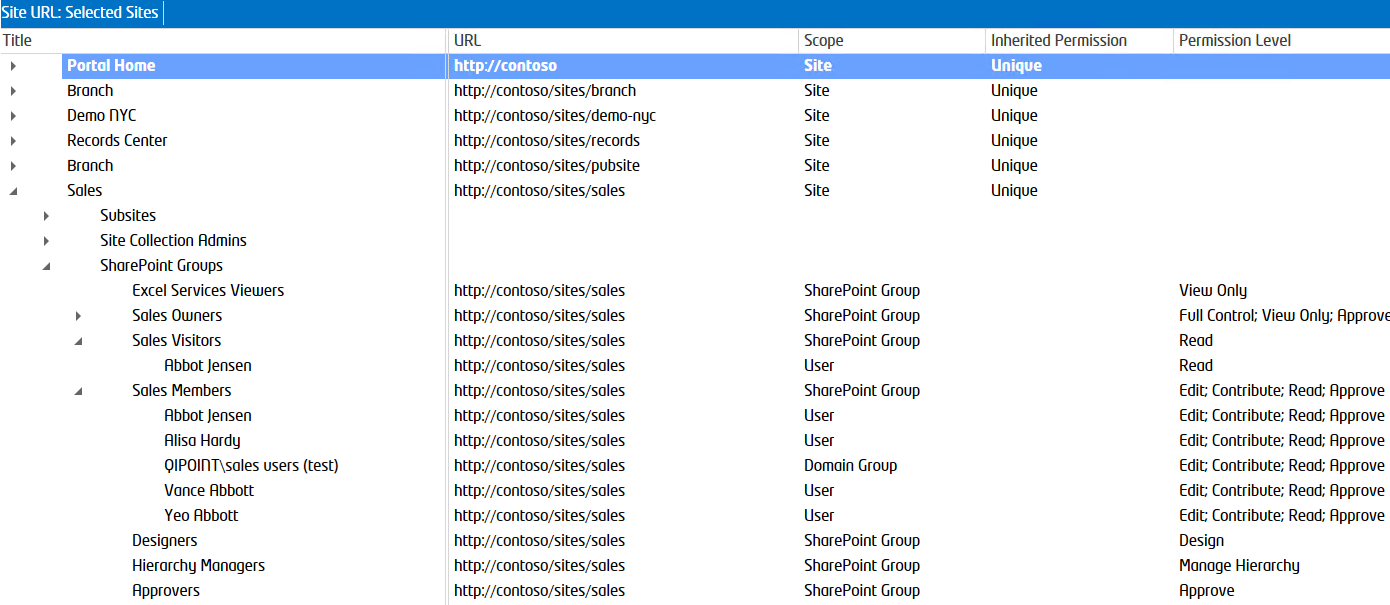
A comprehensive report includes Site, List and Item level permissions in a single report. To get further details you can view the individual reports below for them as well. This report is ‘pre-structured’ so that it is already ‘grouped’ for you.

The comprehensive permission report will show all sites selected in a nested view. Inherited Permissions will not show details of the permissions, they will be listed in the parent object which has Unique Permissions.

An example is shown below:



Looking closer, you will see that Site, List and Item permissions are displayed for multiple Site Collections in a nested view. If further sorting or grouping is needed, you can also open the Site, List or Unique Item Level reports which provides additional grouping abilities not supported in the Comprehensive Report view.



#### Check User 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.

##### Scope

This displays if the permissions granted are at the Site, List, Item or Folder level.

##### Title

This is the Title of the SharePoint Item/object that the account has been granted access to.

##### Name

This is the account name. If this is an Active Directory (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).

##### Email

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

##### URL

This is the absolute URL to the SharePoint Item/Object that the account has access to.

##### 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).

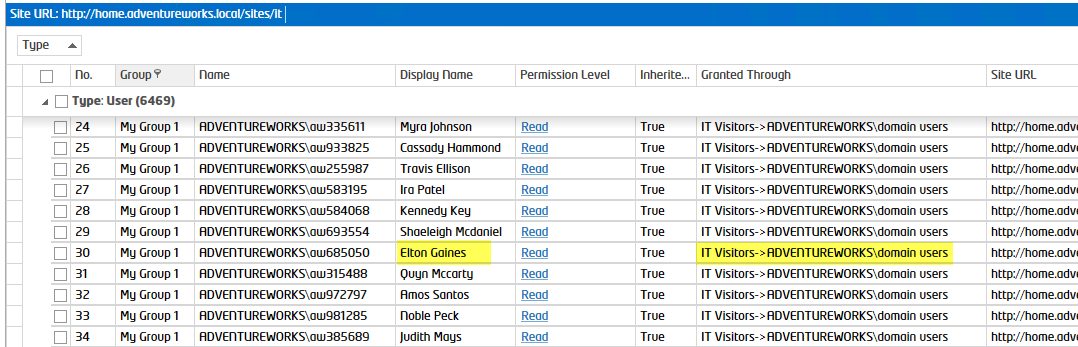
##### Inherited

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” whose access was *Granted Through* a SharePoint Group called “IT Visitors” and the AD Group “Domain Users”:



#### 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

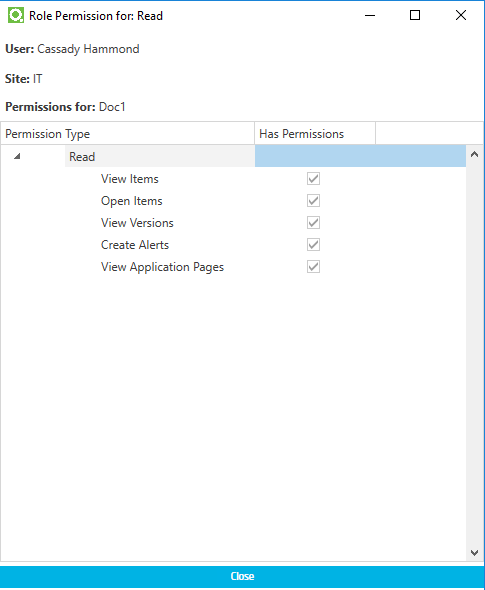
This is the account display name. If this is an AD Account, this will be the Display Name. If this is a SharePoint Group, it will be the Name of the SharePoint Group (which will be the same as Name column above).

##### Email

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

##### 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).

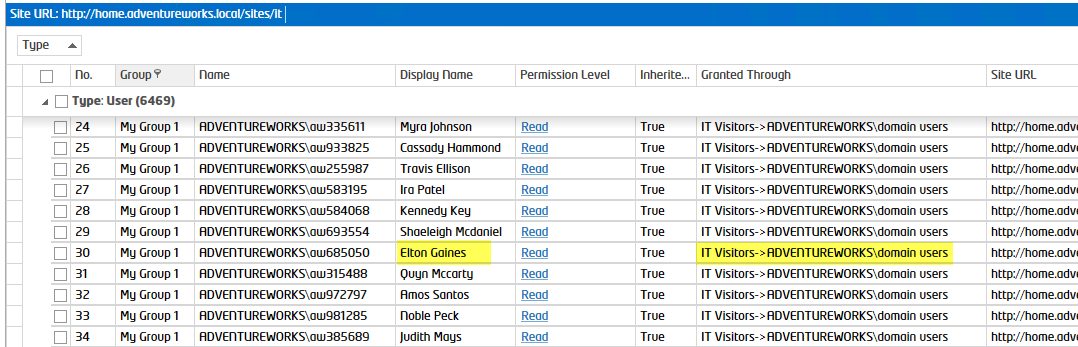
##### Inherited Permissions

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

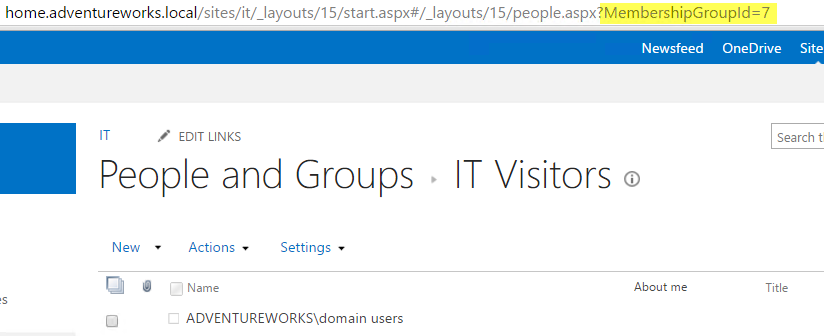
This column will specify how the account (found under column “Name”) was granted access. “Directly Given” = The account was granted access directly to this site, list or item. If this column value is not “Directly Given”, then this account was granted access through a SharePoint Group, an AD Group, or 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” whose access was *Granted 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.

##### Report Date

This is the date that report was generated.

#### 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

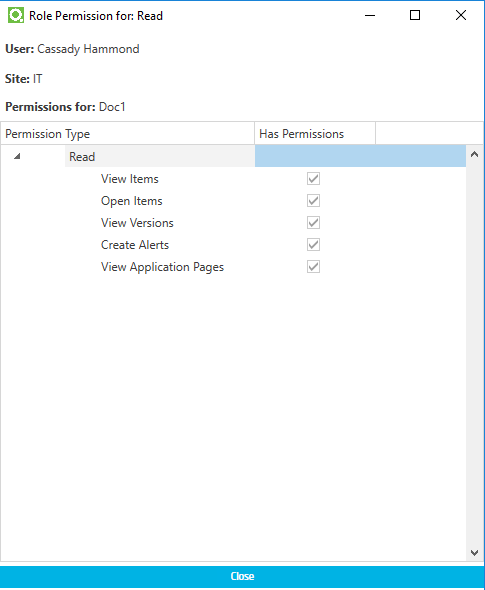
This is the account display name. If this is an AD Account, this will be the Display Name. If this is a SharePoint Group, it will be the Name of the SharePoint Group (which will be the same as Name column above).

##### Email

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

##### 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).

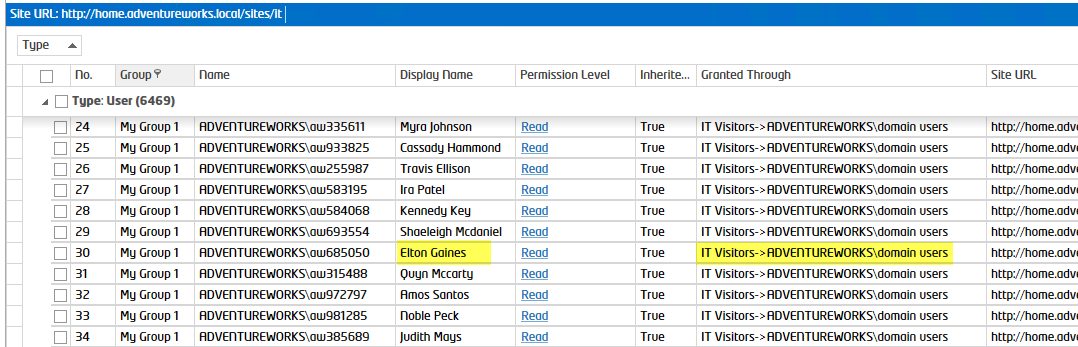
##### Inherited Permissions

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

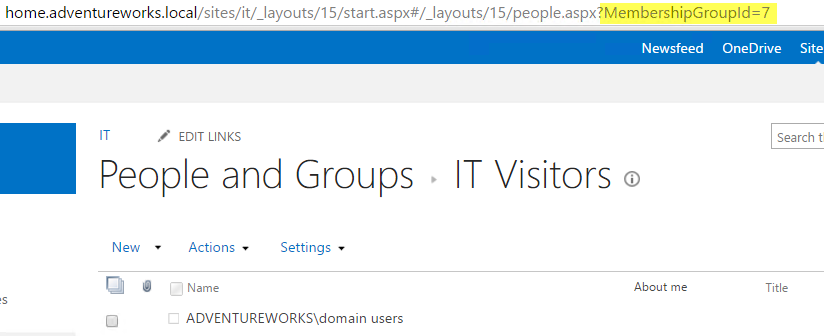
This column will specify how the account (found under column “Name”) was granted access. “Directly Given” = The account was granted access directly to this site, list or item. If this column value is not “Directly Given”, then this account was granted access through a SharePoint Group, an AD Group, or 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” whose access was *Granted 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.

##### 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

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.

##### Report Date

This is the date that report was generated.

#### 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

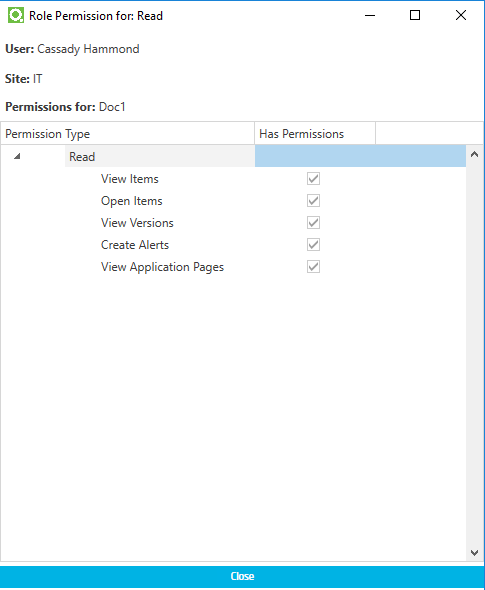
This is the account display name. If this is an AD Account, this will be the Display Name. If this is a SharePoint Group, it will be the Name of the SharePoint Group (which will be the same as Name column above).

##### Email

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

##### 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).



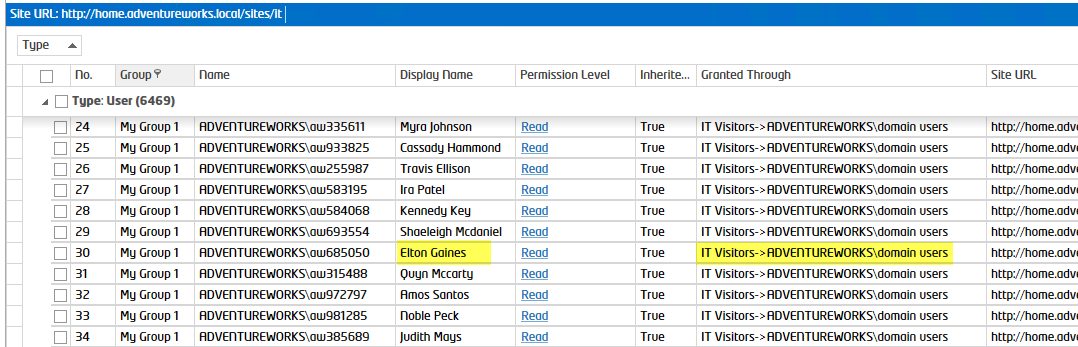
##### Inherited Permissions

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

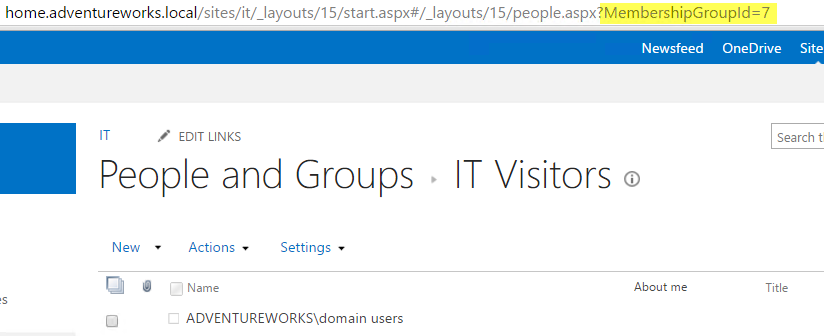
This column will specify how the account (found under column “Name”) was granted access. “Directly Given” = The account was granted access directly to this site, list or item. If this column value is not “Directly Given”, then this account was granted access through a SharePoint Group, an AD Group, or 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” whose access was *Granted 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.

##### 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.

##### 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.

##### Report Date

This is the date that report was generated.

#### 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 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.

##### Report Date

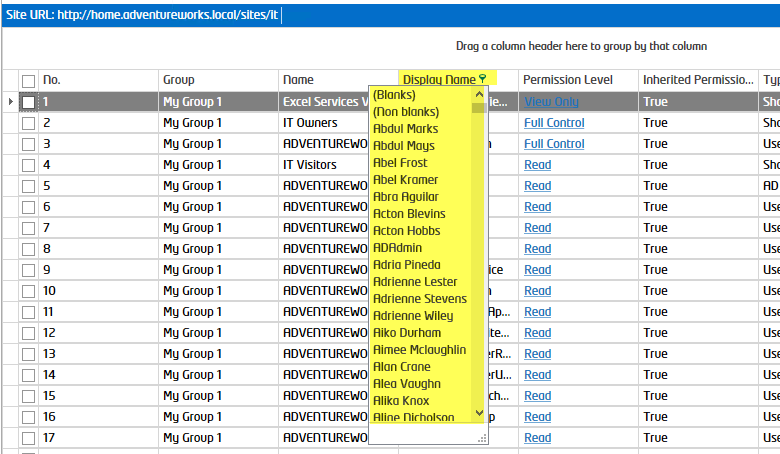
This is the date that report was generated.

# Customizing Permission Reports

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

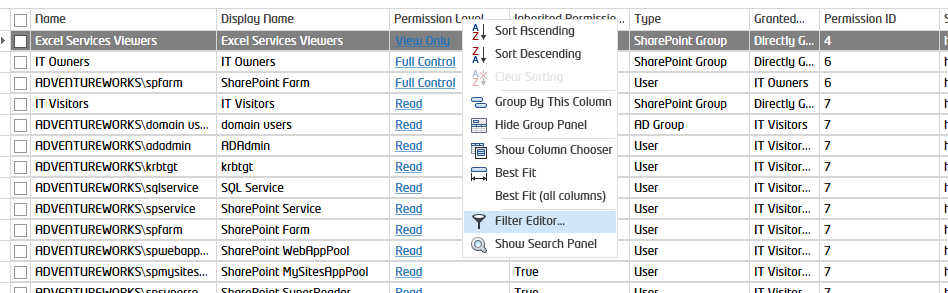
## Filtering

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.

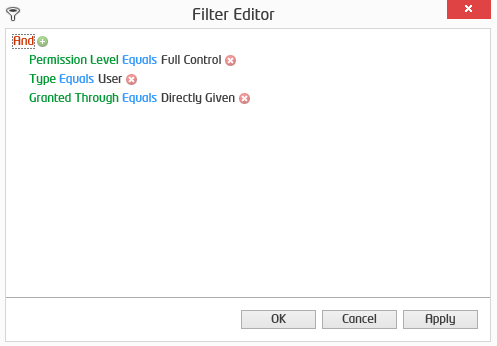


### Advanced Filtering

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



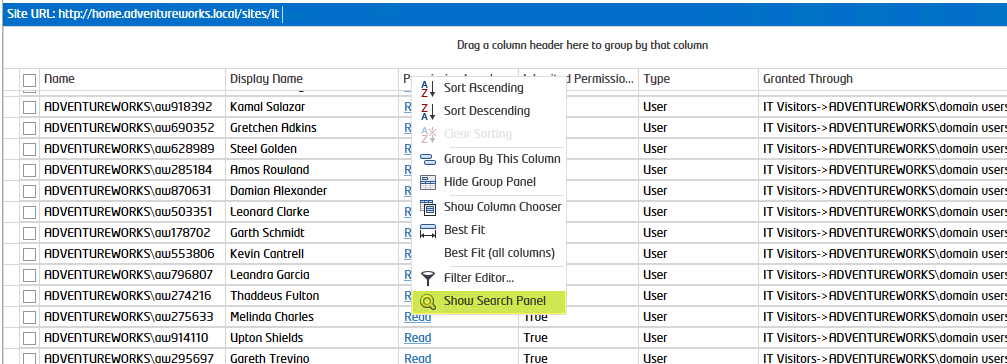
Below is an example of filtering a View to display all areas where a User has been Granted Access directly and has Full Control:



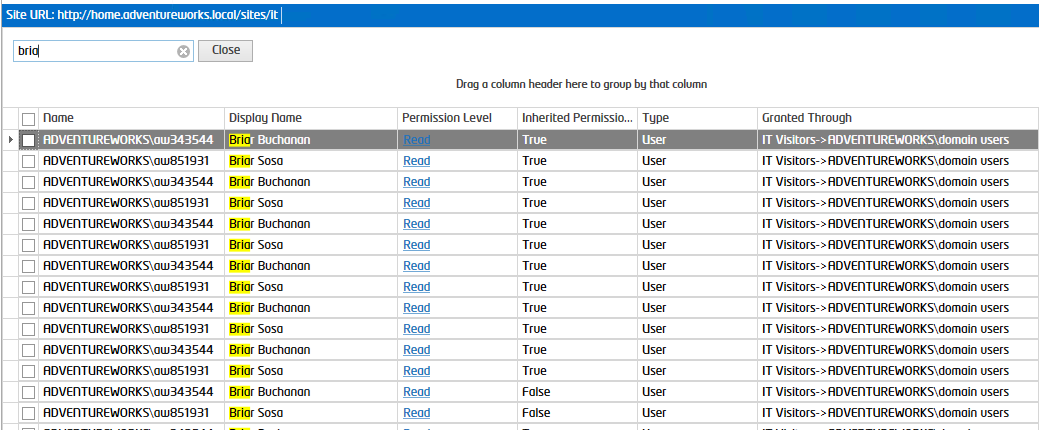
You can apply filters like this and then click “Save View” to re-use it later in other reports.

## Searching within the Report

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



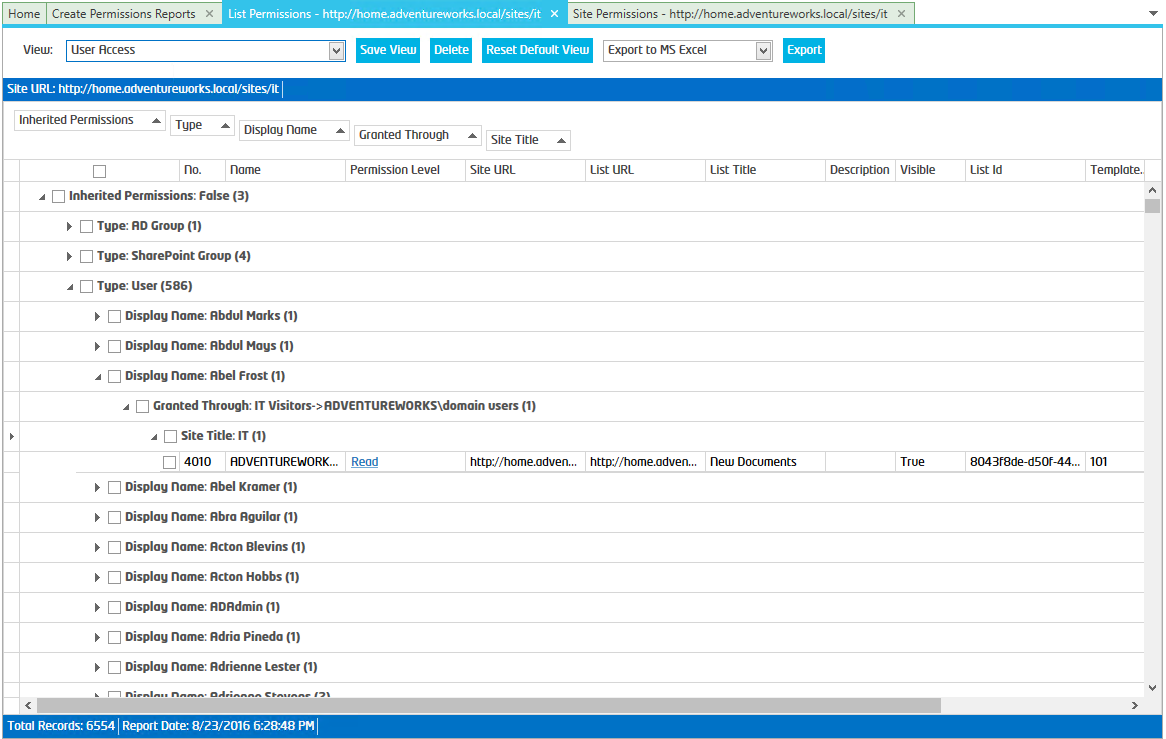
Below I entered “Bria” in the search box and the toolkit will automatically filter results and highlight them in yellow.



## Grouping

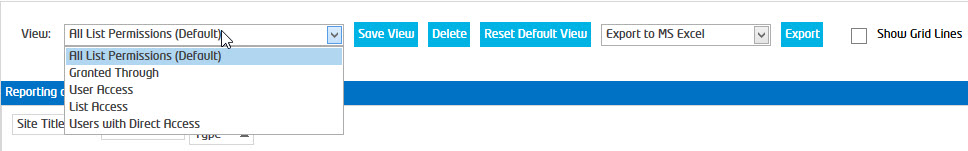
To group the results, drag the column header of the field you want to group by to the top of the results panel. You can also drag multiple panels and rearrange the group ordering by dragging columns left and right of each other.

Below I grouped by “Inherited Permissions” to see all permissions found that are “Unique” and are “Users”:



## Creating “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.

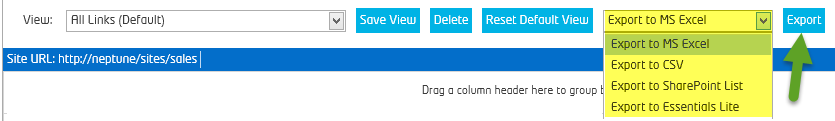


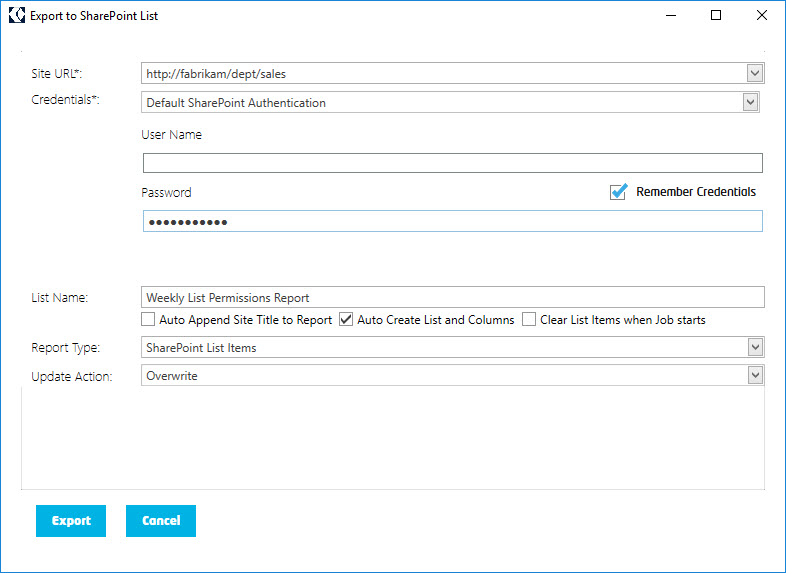
## Export

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. SharePoint Essentials Lite Client (QPCX)

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.





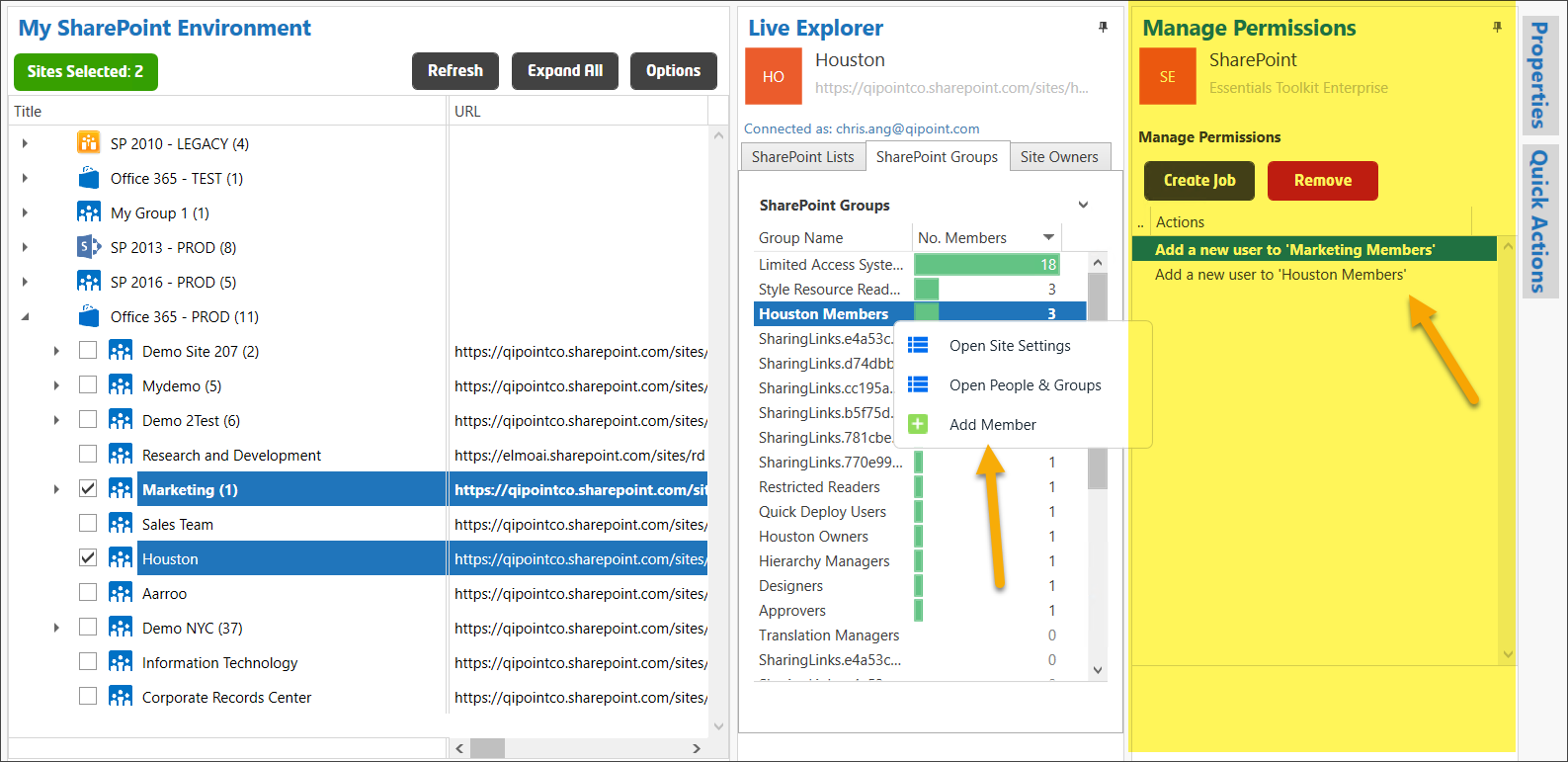
# Permission Templates – “Save Job”

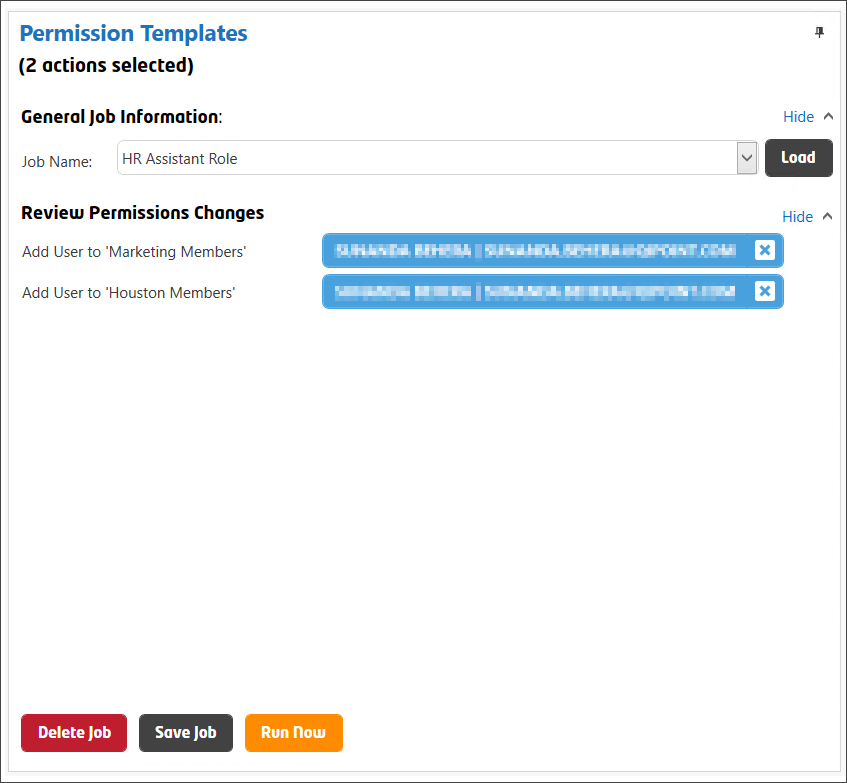
Save Permission Actions (next page) in a ‘Permissions Job Template’

You can use a Permission Report or the Home Page Dashboard to add one or more users to one or more SharePoint Groups.

Once you create a ‘Job’ to add/remove users to groups, you can then save this as a ‘Permissions Job Template’ to re-use later.

For example: I can add a user to 3 different site Members groups, then save this as “HR Assistant Role”. If another employee takes on this role, I can reuse/re-load this template and just change the user to the new employee who started.





# Updating Permissions

## Editing Permissions

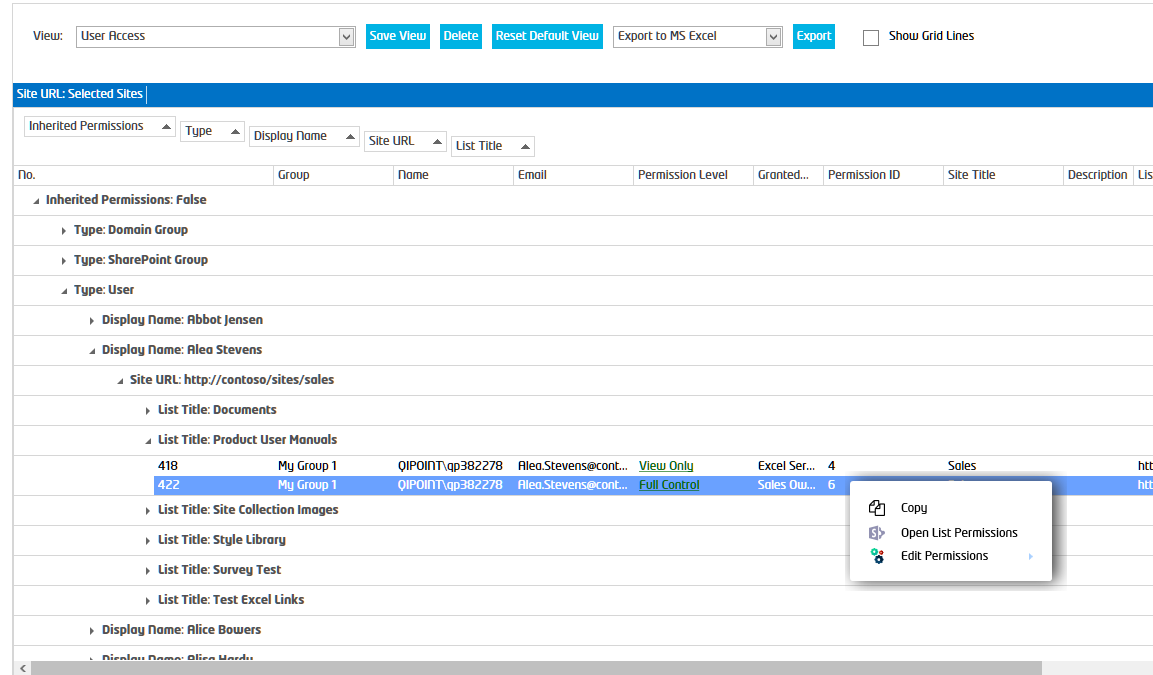
To edit permissions for one or more sites, you first need to run a report on those sites.

You can modify permissions in 2 ways:

* **Manually via SharePoint**: Right click on the report row that you need to modify, and then click Open Item Permissions. Thereafter, you can remove/modify/validate permissions for that report item.
* **Using SharePoint Essentials Toolkit**: Select the report records to modify by selecting the left most column. Right click on a selected row and then select “Edit Permissions”. A window will appear to modify the selected permissions (this will only be visible for objects with ‘Unique Permissions’, Inherited Permissions = False).

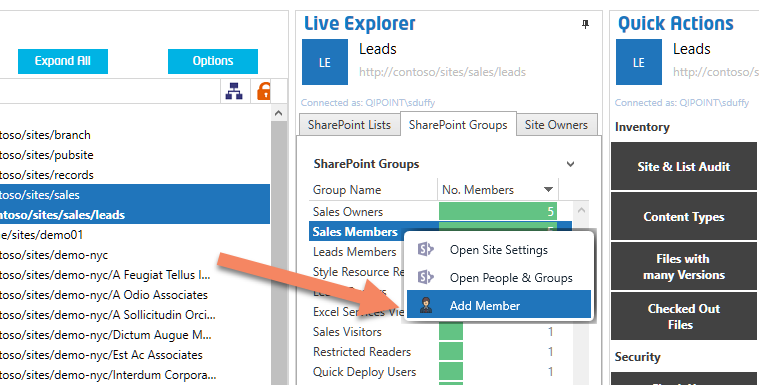
### Manage Permissions: Manually via SharePoint

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.

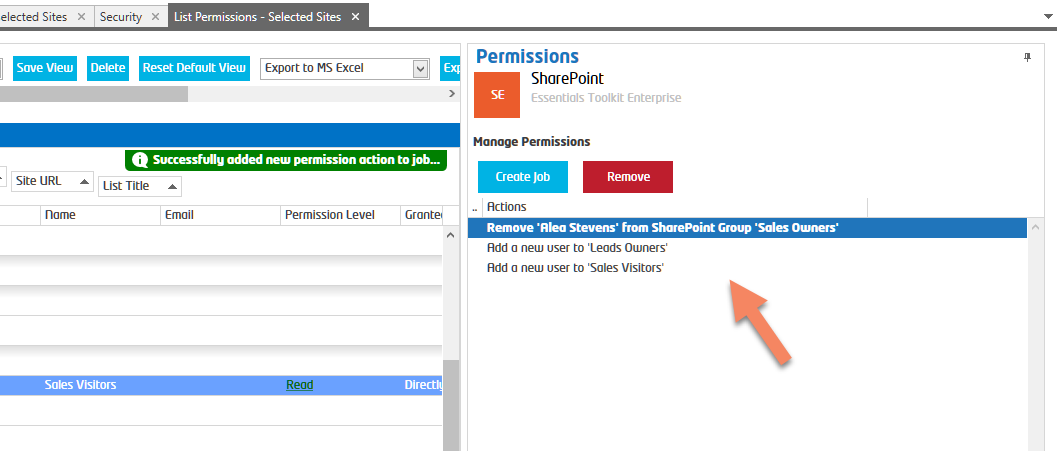


### Manage Permissions: Using SharePoint Essentials Toolkit

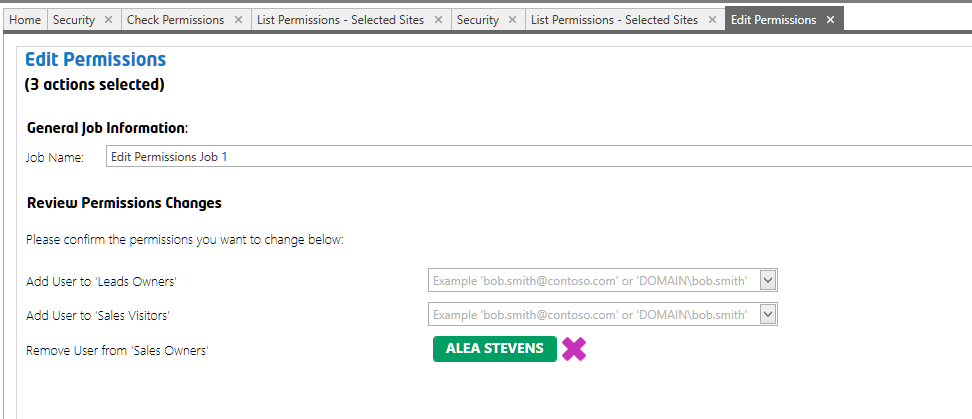
You can add or remove members of a SharePoint Group using the toolkit by right clicking on the Group in the Home Page Dashboard and selecting ‘Add Member’. Or you may use a Permission Report to make permission changes by right clicking on a record.



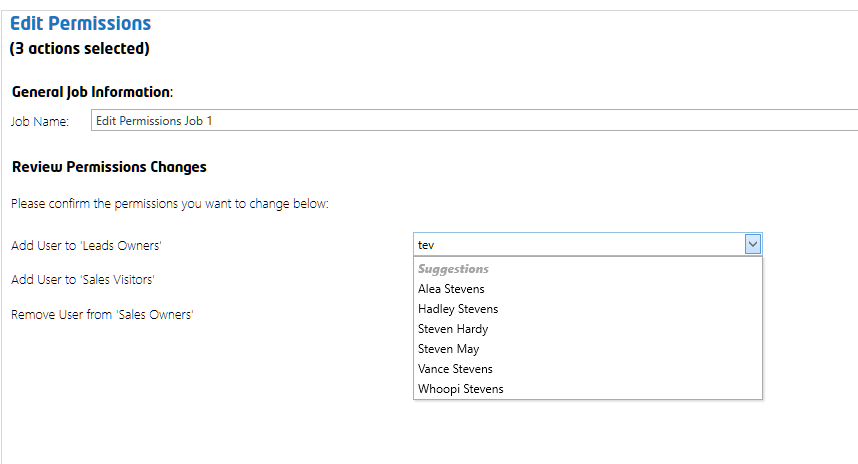
1. From the grid view report right click on a record that has permissions you want to modify, such as a User, and select “Edit Permissions-> (Action)”.
2. The Edit Permissions Panel will open. This will provide a preview of the permissions actions to include in your job.
3. After adding the changes by repeating step 1,2 above, you can then click ‘Create Job’ to create the batch job to perform the permission changes.



1. The Create Job / Edit Permissions page will open. From here you can click ‘Run Now’ after you enter any required information, such as the Users/Groups to add to SharePoint.

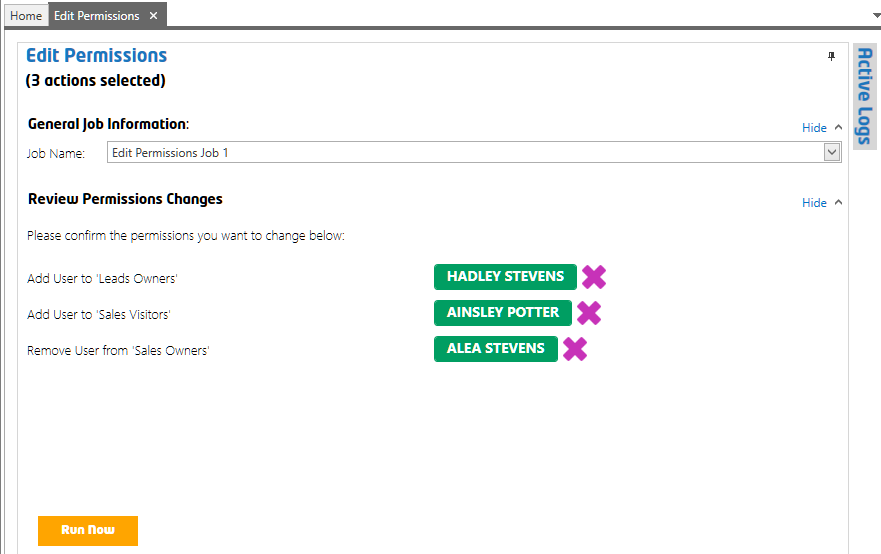


1. Select users from the Suggestions list to complete the entry. Or press the Return/Enter key to confirm an entry:



Entries will show as confirmed when embedded in green ellipse as shown below.

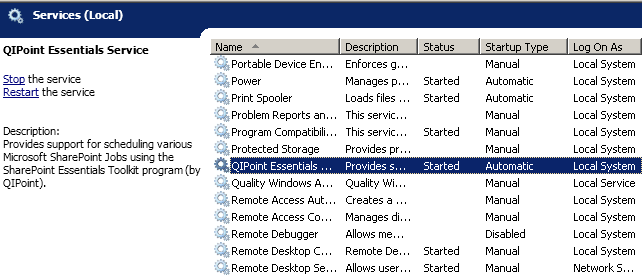
Click the ‘X’ to change an entry.



# Scheduling Jobs

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

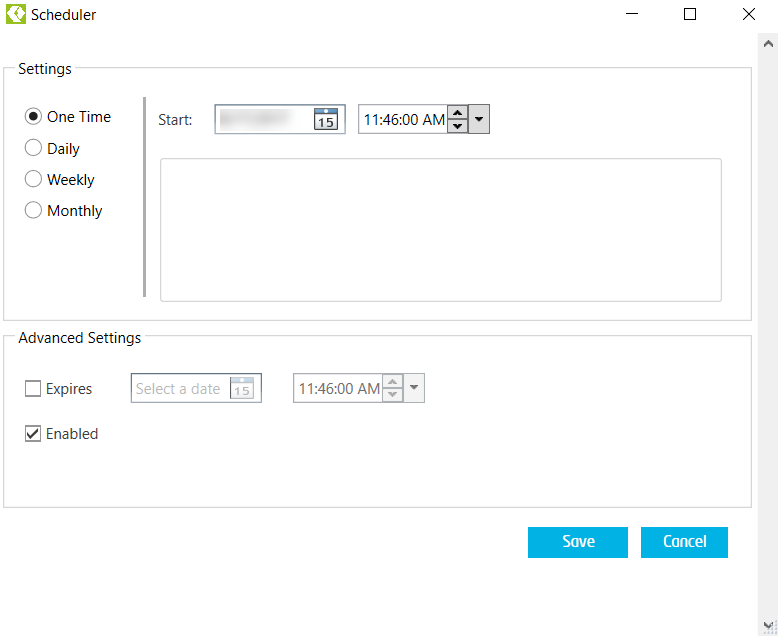
**TIP:** Ensure the “Cognillo Essentials Service” (Windows Service) runs before scheduling a job. Also, make certain the user account (used to run the service) has ‘Modify’ permission to the Report Path (Home -> Settings). By default, this service uses ‘Local System’ which may not have rights to create 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 you are ready to schedule this job. A window will appear to set the date, time and recurrence of the job.

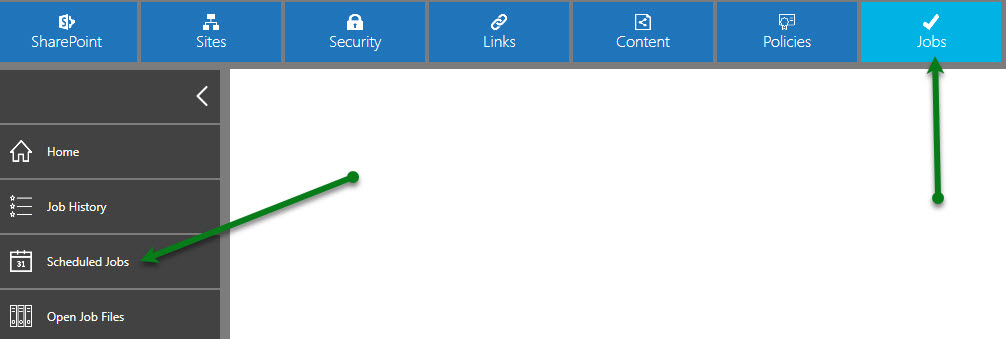


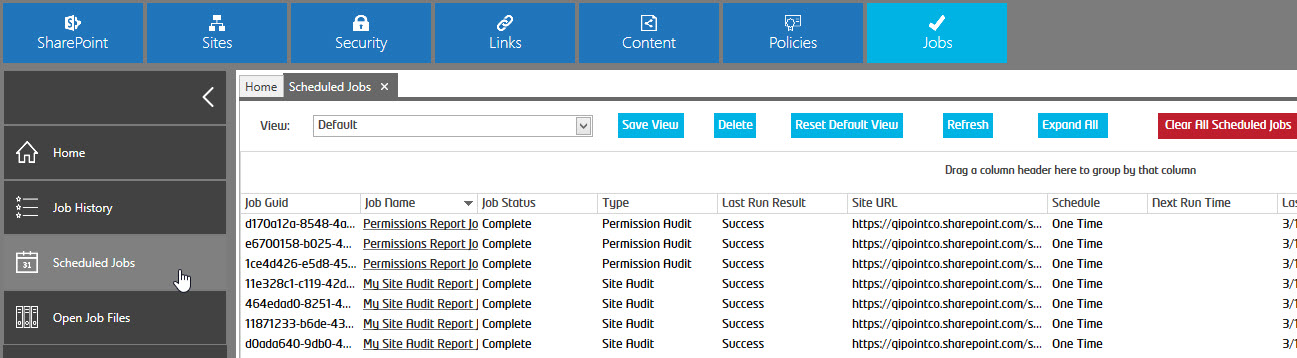


Select the schedule and specific options and then click the Save button to schedule the job.

## List of Scheduled Jobs

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



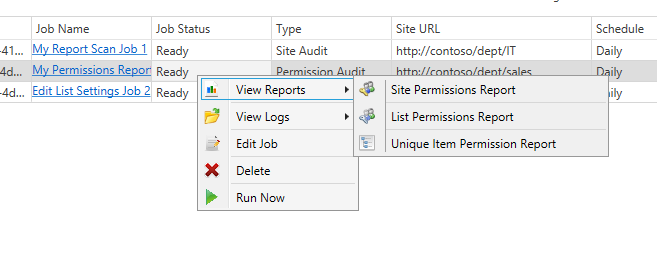


From here you can view reports, logs, execute the job, modify or delete scheduled jobs (by right clicking the job).

## 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, as well as 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 job (this occurs if it is the same site URL that is run 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.

<https://www.cognillo.com/support>

We are here to help!

# Product Features

|  |  |
| --- | --- |
| Feature | Enterprise |
| SharePoint 2010 |  |
| SharePoint 2013 |  |
| SharePoint 2016 |  |
| SharePoint 2019 |  |
| Office 365 |  |
| Searching within Report |  |
| Querying results in the Report |  |
| Personalize Permission Reports using “Views” |  |
| Report Site, List and Item Level Permissions |  |
| Report Permissions across Farms & Site Collections |  |
| Include SharePoint Group Nested Permissions |  |
| Include AD Group & Azure 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 |  |
| Share Report “Views” with other users |  |
| Report on Sharing Links |  |
| Edit Permission Objects in Bulk |  |
| Email results automatically to users |  |
| Schedule Jobs & Report Generation |  |
| Export Reports to SharePoint List |  |
|  |  |