Copyright

© Metalogix International GmbH., 2008-2016
All rights reserved. No part or section of the contents of this material may be reproduced or transmitted in any form or by any means without the written permission of Metalogix International GmbH.

ControlPoint™ is a trademark of Metalogix International GmbH.

Windows SharePoint Services is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

Technical Support

For information about Metalogix Technical support visit http://metalogix.com/support.

Technical support specialists can be reached by phone at 1.202.609.9100.

The level of technical support provided depends upon the support package that you have purchased. Contact us to discuss your support requirements.
Contents

Getting Started with ControlPoint 7

Launching ControlPoint Online................................................................. 7
The ControlPoint Configuration Site......................................................... 7
Using Discovery to Collect Information for the ControlPoint Database Cache................................................................. 9
   Nightly Full Discovery O365.................................................................. 9
Running Discovery from the ControlPoint Application Interface...................................................................................... 10
The ControlPoint Interface..................................................................... 11
Icons.......................................................................................................... 12
ControlPoint Left Navigation Panels...................................................... 14
   SharePoint Hierarchy........................................................................... 14
   Manage ControlPoint.......................................................................... 14
   Search.................................................................................................. 15
   Displaying ControlPoint Menus in a Ribbon........................................ 16
The ControlPoint Application Header....................................................... 17
   Opening a ControlPoint Workspace in a New Window or Tab.................. 18
   Signing Into ControlPoint as Another User............................................ 18
Selecting Objects on Which to Perform a ControlPoint Operation ................. 19
   The Workspace Selection Section......................................................... 21
   Changing Your Selection.................................................................... 22
   Selecting List Items on Which to Perform a ControlPoint Operation........ 27
   Adding Objects from the SharePoint Hierarchy to Your Selection........... 30
   Saving and Re-Using a SharePoint Object Selection................................ 30
Selecting Users on Which to Perform a ControlPoint Action or Analysis ......... 32
   Selecting Individual Users................................................................... 33
   Operations that Include Two People Pickers........................................... 33
   Refreshing the SharePoint Hierarchy...................................................... 33
   Refreshing the SharePoint Hierarchy Cache............................................ 34

Searching for SharePoint Sites ................................................................. 35
   Performing a Simple or Advanced Search............................................ 35
Data Analysis and Reporting

Specifying Parameters for Your Analysis ................................................................. 93
Analysis Results Display .......................................................................................... 97
Working with Data Analysis Results ...................................................................... 99
   Linking to SharePoint Pages and Other ControlPoint Analyses from Analysis Results ........................................... 100
   Acting on Search or Data Analysis Results ......................................................... 101
Generating a SharePoint Summary Report ............................................................... 103
Analyzing Site Collection Storage ......................................................................... 105
Analyzing Storage by File Type ............................................................................. 108
Analyzing Trends .................................................................................................... 110
Analyzing Managed Metadata Usage .................................................................... 112
Analyzing Users and Permissions ......................................................................... 115
   Finding Orphaned Domain Users .................................................................... 115
   Analyzing Site Permissions .......................................................................... 118
   Analyzing Site Lists Permissions ................................................................. 120
   Analyzing Permissions by List Item ............................................................... 122
   Analyzing Comprehensive Permissions ......................................................... 124
   Analyzing SharePoint Groups ....................................................................... 125
Auditing Activities and Changes in Your SharePoint Environment .................... 128
   Events Captured in SharePoint Logs .............................................................. 128
   Analyzing Audit Log Contents ...................................................................... 130
   Analyzing Change Log Contents .................................................................... 133
The ControlPoint Task Audit .................................................................................. 135
   Viewing Logged Errors ................................................................................... 138
Analyzing List Properties ....................................................................................... 139
Generating a OneDrive Summary Report ............................................................... 142

Scheduling a ControlPoint Operation

Scheduling a Recurring Analysis for Which a Specific Date
Range or Time Period was Selected ........................................................................ 144
How Scheduled Jobs are Handled ......................................................................... 146
Creating a Scheduled Job ...................................................................................... 146
Monitoring Scheduled Jobs .................................................................................. 149
   Viewing/Editing a Scheduled Job ................................................................... 152
   Viewing a Scheduled Job's History ............................................................... 153
Canceling or Deleting a Scheduled Job ................................................................. 154
Updating Full Discovery and Scheduler Windows Jobs ...................................... 155
Generating a Scheduled Jobs Report ................................................................. 156

Saving, Modifying and Executing Instructions for a ControlPoint Operation 159
Saving Instructions ......................................................................................... 159
Modifying Instructions ................................................................................... 159
Executing Instructions ..................................................................................... 160

Analyzing SharePoint Content for Compliance 162
Compliance Administrators and Quarantine Administrators
Groups ........................................................................................................... 163
Registering with Metalogix Cloud Services ..................................................... 163
Compliance Action Severity Levels ................................................................. 163
Defining Compliance Action Rules ................................................................. 164
Submitting Content to Metalogix Sensitive Content Manager
for Compliance Analysis ................................................................................ 168
Managing Compliance Actions ....................................................................... 169
  Reclassifying Items Returned as Unable to Classify .................................... 174
  Managing Quarantined Items ....................................................................... 175
Reporting on Sensitive Content Activity ......................................................... 176

Using ControlPoint Sentinel to Detect Anomalous Activity 180
How Personal Daily Activity is Determined ................................................... 180
Defining Business Hours for Anomalous Activity Detection......................... 181
Defining Base Line Rules for Anomalous Activity Detection.......................... 182
Defining Anomalous Activity Rules ................................................................. 184
Preparing Your Environment for Using ControlPoint Sentinel ...................... 185
Reporting Anomalous Activity ....................................................................... 188
Getting Started with ControlPoint

Metalogix ControlPoint is a Web-based tool that runs as a SharePoint application and facilitates the management of multiple SharePoint objects (Web applications, site collections, sites, lists, libraries, and items) and users within a SharePoint farm. In addition to enabling you to navigate throughout a SharePoint farm using a single interface, ControlPoint offers a number of powerful search and data analysis tools as well as value-added features not currently available in native SharePoint.

Launching ControlPoint Online

Use one of the following options to launch the ControlPoint Online application.

From your workstation browser:

Enter http://<machine_name>:<port_number>/_layouts/axceler/xcmain.aspx.

(The server machine name is the name of the machine on which the ControlPoint client application is installed. 2828 is the default port number for the MetalogixOnline application pool.

NOTE: If you are a ControlPoint Application Administrator logging in for the first time, complete the login screen using the account that was designated as the ControlPoint Site Collection Administrator account at the time the ControlPoint Online application was installed.

From the machine on which ControlPoint Online has been installed:

1. Log into the server using the account that was designated as the ControlPoint Service Account at the time the ControlPoint Online application was installed.
2. From the Windows Start menu, choose Programs > Metalogix > ControlPoint_Online> Launch ControlPoint Online Application.

The ControlPoint Configuration Site

The ControlPoint Configuration site is a SharePoint site that is integral to your ControlPoint Online installation.

This site is used primarily for managing ControlPoint users and permissions and configuring menus that display in the ControlPoint left navigation pane. To manage groups you either need direct rights to manage the groups or be a site collection administrator.

If you are a site collection administrator for the ControlPoint Configuration site collection, you can access the site's administration pages and ControlPoint value-added features from the SharePoint Hierarchy panel. See “ControlPoint Security” for more detail.
If you have sufficient permissions (regardless of whether you are the site collection administrator), you can access the site's home page:

- from the SharePoint Hierarchy panel, by right clicking the ControlPoint Configuration Site - Root Site and choosing Open Site.

- from the Manage ControlPoint panel by choosing ControlPoint Configuration > ControlPoint Configuration Site.
Using Discovery to Collect Information for the ControlPoint Database Cache

Discovery is a background task that collects information and stores it in the ControlPoint Services (xcAdmin) database cache for use in ControlPoint data analysis and reporting.

Nightly Full Discovery O365

As part of the initial configuration of ControlPoint Online, the nightly Full Discovery tasks is created in Windows Task Scheduler on the server where ControlPoint Online is installed.

If ControlPoint was installed for the first time with version 5.3 or higher, the nightly Discovery job is disabled by default, as are operations and parameters that rely on cached data collected by Discovery.

You can activate the Nightly Full Discovery task and change the default start time and/or frequency via the Schedule Monitor Windows Jobs view.
Running Discovery from the ControlPoint Application Interface

A manual Discovery can also be run from the ControlPoint application interface, which can be useful:

- when you want to update the ControlPoint cache for specific site collections only without having to run a more resource-intensive Full Discovery.
- for site collections that have been excluded from the Full Discovery process. For example, exceptionally large site collections can greatly increase the Full Discovery run time. Site collections containing such sites may be excluded from the Full Discovery process and scheduled to run less frequently. Details on how to exclude Web applications and/or site collections from Full Discovery can be found in the *Metalogix ControlPoint for Office 365 Administration Guide*.

**NOTE:** You can run Discovery only on site collections for which you are a Site Collection Administrator.

By default, operations that rely on data collected by Discovery are disabled. Once Discovery is run, these operations can be enabled via the ControlPoint Setting *DiscoveryEnabled*. Refer to the *ControlPoint for Office 365 Administration Guide* for details.
To run Discovery from the ControlPoint application interface:

1. From the Manage ControlPoint panel choose ControlPoint Management > Discovery.

2. Use the information in the following table to determine the appropriate action to take.

<table>
<thead>
<tr>
<th>If you want run a...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Discovery</td>
<td>do not modify the Selection section. REMINDER: Only site collections for which you have Site Collection Administrator privileges will be included in the scope of the action.</td>
</tr>
<tr>
<td>Partial Discovery</td>
<td>select the site collection(s) on which you want to run Discovery, using the procedure for Changing Your Selection. NOTE: The Partial Discovery will include all site collections that you explicitly select, regardless of whether they have been excluded from the nightly Full Discovery process.</td>
</tr>
</tbody>
</table>

3. Either:
   - run the Discovery immediately (by clicking the [Run Now] button).
   OR
   - schedule the Discovery to run on a one-time or recurring basis (see Scheduling a ControlPoint Operation).

The ControlPoint Interface

The ControlPoint interface employs a two-pane design. From the left (navigation) pane, you can select the SharePoint object(s) on which you want to operate and initiate the operation. The right (workspace) pane is where the feature you choose is displayed.

Whenever you log into ControlPoint or refresh your browser, the right pane displays a dashboard which includes:

- statistical information about your SharePoint farm

NOTE: This information is updated whenever you log in, as well as whenever the ControlPoint
application pool is restarted.

- quick links to some of ControlPoint's most powerful functionality:
  - the Site Permissions Analysis, which lets you examine the permissions that users have for selected sites
  - the Audit Log Analysis, which lets you view selected events written to the SharePoint Audit Log
  - the Site Collection Storage Analysis, which provides storage statistics for selected site collections
  - the Set User Direct Permissions action, which lets you grant users direct permissions to one or more SharePoint sites, lists/libraries, and/or items
  - the Duplicate User Permissions action, which lets you copy the permissions of one SharePoint user to one or more others
  - the Delete User Permissions action, which lets you delete SharePoint user permissions from one or more site collections/sites

- links to the Metalogix Customer Portal as well as ControlPoint user documentation on the Metalogix website.

If a ControlPoint operation is launched from the dashboard, you must select the object(s) on which to perform the operation using the Change Selection option.

Icons

ControlPoint uses the following icons to identify items that display in the left navigation pane.
<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Home" /></td>
<td>The SharePoint virtual <strong>Farm</strong></td>
</tr>
</tbody>
</table>
| ![Search](image) | A ControlPoint **Search** feature  
See Also [Searching for SharePoint Sites](#). |
| ![Folder](image) | A grouping of **SharePoint items** (such as lists, groups, or users) |
| ![Folder](image) | A SharePoint **Site collection**  
**NOTE:** Icons for which you are not a site collections administrator will appear grayed out. |
| ![Folder](image) | A Site collection's **root site** |
| ![Folder](image) | A SharePoint **Site** or **Subsite** whose permissions are **inherited** from its parent |
| ![Folder](image) | A SharePoint **Site** or **Subsite** whose permissions are **unique** (or not inherited) |
| ![Folder](image) | The node under which **OneDrive (Personal) Site Collections** are displayed. |
| ![Folder](image) | A **OneDrive (Personal) Site Collection**  
To optimize SharePoint Hierarchy load time, OneDrive site collections are excluded by default. To use ControlPoint to manage these site collections, ControlPoint Site Collection Administrators must explicitly choose to include them. (Keep in mind that doing so may significantly increase SharePoint Hierarchy load time, especially if there are a large number of OneDrive site collections in your environment.) Contact [Metalogix Support](#) for details. |
| ![List](image) | A SharePoint **List**  
**NOTE:** Variations of this icon are used to represent different types of lists (Document Libraries, Calendars, Announcements, and so on). |
| ![User](image) | SharePoint **Users** |
| ![Group](image) | SharePoint **Groups** |
| ![Gear](image) | A ControlPoint **value-added action** |
| ![Page](image) | A SharePoint **page** |
| ![Analytics](image) | A ControlPoint value-added (**Visual Analytics**) analysis. |
ControlPoint Left Navigation Panels

The standard ControlPoint left navigation frame consists of the following tabs:

- Hierarchy
- Manage
- Search Hierarchy

SharePoint Hierarchy

When Hierarchy is selected in the left navigation frame, you can access the core functionality for managing your SharePoint environment. The navigation tree is designed so that you can visualize the hierarchy of the farm, including:

- the site collections, sites, and subsites managed by ControlPoint Online
- within each site, its associated lists, groups, and individual users.

NOTE: Only site collections for which you are a Site Collection Administrator are visible.

From most levels of the hierarchy you can invoke a right-click menu and access SharePoint pages and ControlPoint value-added features.

Manage ControlPoint

When the Manage tab is selected from in the left navigation frame you can access:

- tools for executing and reporting on ControlPoint operations, and
• depending on your permissions, tools for Managing ControlPoint Configuration and Permissions.

Search

When Search is selected in the left navigation frame, you can easily locate site collections, sites, and subsites within your SharePoint Farm.

You can access this menu directly or from any of the Search Hierarchy links within the SharePoint
Hierarchy panel. For more detail, see Searching for SharePoint Sites.

**Displaying ControlPoint Menus in a Ribbon**

By default, ControlPoint is configured to allow menus to be displayed as right-click context menus in the left navigation frame and ribbon-style menus in the application header. (ControlPoint Application Administrators can, however, configure the application to allow only one or the other.)

**NOTE:** Whenever you change how menus are displayed, the ControlPoint application will automatically restart.

**To display (hide) the ribbon:**

If you are using Internet Explorer 8 or 9, turn Compatibility View OFF to ensure the ribbon will render properly.

From the SharePoint Hierarchy farm node, right-click and choose Refresh with Ribbon On (Off).
To display (hide) context menus:

From the ribbon Home tab, choose Refresh with Context Menus On (Off).

The ControlPoint Application Header

The bottom of the left navigation frame contains:

- The **Available Farms** drop-down that identifies the farm currently being managed and, in a multi-farm installation, lets you select a different farm to administer.
  
  Note that only farms that share the same ControlPoint Service database will be available from the drop-down.

  **NOTE:** Initially, the list includes the names of all farms that have been configured to share the same ControlPoint Service database. However, after the first server interaction (for example, when a ControlPoint action or analysis is initiated), the list may be trimmed to display only farms that are currently active.

- Access to information **About** the ControlPoint application, including:
  
  - the current version, and
  
  - the number of Web front-end servers that are licensed as well as the license status.

  **NOTE:** **Last Patch** reflects the date of the last software update provided by Metalogix. **Last Install** reflects the last full build of that version released by Metalogix.
A link to ControlPoint online Help (3).

Opening a ControlPoint Workspace in a New Window or Tab

You can create a dedicated workspace for a particular task by opening it in a separate window or tab (depending on your browser version). This enables you to navigate to other areas of the ControlPoint interface without having to navigate away from a task in progress. You can even create workspaces to manage multiple ControlPoint operations simultaneously.

NOTE: You invoke the workspace after you have selected a function, but before you have entered data, taken an action, or displayed results. (That is, the new workspace will only display a function in its initial state.)

To open a ControlPoint workspace in a new window or tab:

1. Select the object(s) on which you want to perform an operation.
2. Choose the applicable menu option.
3. From the ControlPoint application header, click the Clone Work Area icon ( ).

Signing Into ControlPoint as Another User

If you have sufficient permissions, you can sign into ControlPoint as a different user, with the access levels and menu permissions that have been set up for that user on the ControlPoint Configuration site. This feature is useful if you want to log into ControlPoint from a workstation other than your own.

To sign into ControlPoint as a different user:

1. From the user name drop-down in the ControlPoint application header, choose Sign in as Different User.
2 Enter the new log in credentials in the Connect to [server] dialog.

![Log In dialog]

3 Use the information in the following table to determine the appropriate action to take.

<table>
<thead>
<tr>
<th>If you ...</th>
<th>Then ...</th>
</tr>
</thead>
</table>
| check **Remember my password** | the new account credentials will:  
  • display in the ControlPoint application header, and  
  • be used for:  
    ▪ all ControlPoint functionality (searches, actions, and analyses), and  
    ▪ SharePoint pages accessed from within ControlPoint.  
  
  **WARNING:** If you use this option to log into another user’s workstation, remember to ensure that the password is properly cleared when you are finished, either by logging in as the workstation user with "Remember my password" checked, or by using browser functions to clear saved passwords. |
| leave **Remember my password** unchecked | • the new account credentials will:  
  ▪ display in the ControlPoint application header, and  
  ▪ be used for all ControlPoint functionality (searches, actions, and analyses), and  
  ▪ the account credentials associated with the original workstation login may continue to be used for SharePoint pages accessed from within ControlPoint.  
  
  If you use this option and want to access a SharePoint page under the new account credentials, you can, of course, use the Sign In as a Different User option from within the SharePoint page. |

### Selecting Objects on Which to Perform a ControlPoint Operation

#### Selecting Objects from the SharePoint Hierarchy, Favorites, or Search Hierarchy Panel

From the SharePoint Hierarchy, Favorites, or Search Hierarchy panel, you can select one or more objects on which to perform a ControlPoint search, action, or analysis. You can select the entire farm, individual site collections, sites, lists, and/or users.
To select multiple objects, hold down either the [Ctrl] or [Shift] key and left-click on each item you want to include in your selection. (To clear all selected object(s), left-click on any item that is not currently selected.)

After selecting the object(s):

- if context menus are enabled, right-click to display a menu from which you can choose the operation you want to perform.

OR
• if the ribbon is enabled, select from the appropriate tab in the ribbon and choose the operation you want to perform.

![Ribbon of ControlPoint](image)

**NOTE:** The level of the hierarchy from which you select the object(s) determines the options available and the scope of the operation. For example, you can select objects at different levels of the hierarchy if the operation allows it. If you attempt to select objects from different levels when an operation does not allow it (for example, you have selected both site collections and sites then try to initiate a Site Collection Property Report), only the relevant objects will apply. Similarly, if you select multiple objects then choose an option that is only valid for a single object (such as copying or moving a site), only the object on which you right-click will apply.

If you selected an operation that can be performed on items within a list, select the list(s), choose the operation, then follow the procedure for Selecting List Items on Which to Perform a ControlPoint Operation.

**Selecting Items from Search or Data Analysis Results**

You can also select one or more objects on which to perform an operation from simple/advanced search or data analysis results. For details, see Acting on Search or Data Analysis Results.

**The Workspace Selection Section**

Once you have initiated a ControlPoint operation, the object(s) you selected display in the Selection section of the workspace. Information that displays in the Selection table includes an icon identifying the item's Type (that is, farm, Web application, site collection, or site/subsite) and the URL.
Generally, if you selected at the farm, Web application, or site collection level, all child items are included by default, as indicated by a check mark (✔) in the Include Children column. Because these items are simply "containers" for the actual sites and subsites on which you want to perform the operation (that is, for most operations you cannot act on these items themselves), the assumption is that if you selected at one of these levels you intended to include all children.

### Changing Your Selection

After selecting objects on which to perform a ControlPoint operation, you can add or remove objects using the Change Selection feature.

**NOTE:** If you chose an operation designed to work on a single object (such as Copy/Move), the Change selection option will not be available.

You can also add individual objects to your current selections using the Add to Selection menu item. See [Adding Objects from the SharePoint Hierarchy to Your Selection](#).

### To access the Change Selection pane:

In the Selection section of the work area, click the Change selection icon ( ).

The Change Selection pane displays, which consists of two sections:

- the Available Items section lists all of the objects available for selection (as determined by the scope of your original selection)
- the Selected Items section lists currently-selected objects.
Typically, all child items (site collections, sites, and subsites) are included in the scope by default, as indicated by a check mark to the left of the item in the Selected Items section.

The level to which you can drill down in the Available Items list depends on the action that you want to perform.

EXAMPLES:
If you chose **Set Site Collection Properties** which, by definition, applies only to site collections, you cannot drill down beyond the site collection level.

*Set Site Collection Properties ➤ Select scc*
If you chose **Set Site Properties**, you can drill-down and select individual sites within the collection.

To modify the list of available items:

Use the information in the following table to determine the appropriate action to take.

<table>
<thead>
<tr>
<th>If you want to ...</th>
<th>Then ...</th>
</tr>
</thead>
</table>
| expand the scope of available items to encompass the farm | check the **Expand Scope** box.  
   | NOTE: If you originally selected the farm, multiple Web applications, or site collections within multiple Web applications, **Expand Scope** is checked by default and all available items in the farm display. |
| narrow the scope of available items | • enter a full or partial site **Name** and/or **URL**, and  
   • click the magnifying glass icon (🔍).  
   | NOTE: By default, ControlPoint uses real-time data for this type of hierarchical search. However, to enable faster searches in large environments, ControlPoint Application Administrators can configure the application to use cached data for hierarchical searches. |
To modify the Selected Items list:

1. Uncheck the "include all children" box to the left of each object whose scope you want to modify.

2. In the Available Items list, select each object that you want to include. Use the information in the following table for guidance.

<table>
<thead>
<tr>
<th>If you want to ...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>select multiple items individually</td>
<td>hold down the [Ctrl] or [Shift] key and highlight each item you want to add.</td>
</tr>
<tr>
<td>immediately add an item and all of its children to the Selected Items column</td>
<td>highlight the item, then right-click and choose Add Item and All Children.</td>
</tr>
</tbody>
</table>
| select an item and its immediate children (for example, a site collection and its root site only) | highlight the item, then right-click and choose Highlight Immediate Children. (If objects are grouped into a folder, you must first expand the folder.)  

TIP: You can use this option as a time-saver if you want to add most, but not all of the selected child items. After highlighting the item you can then individually de-select those that you want to exclude.

3. To add the highlighted item(s) to the selection list, do one of the following:
   - drag and drop the item(s) to the Selected Items column. ControlPoint will automatically place them in the correct location in the tree.
   - click the [Add] button.

Note that if a checkbox displays to the left of a selected item (indicating that you want to include all child items), those child items do not display explicitly in the Selected Items list.
If you uncheck this box then add child items using the procedure above, however, each item you add will display explicitly in the list.

![Selected Items Diagram]

To remove items from the Selected Items list:

1. In the Selected Items list, highlight each item that you want to remove. Hold down the [Ctrl] or [Shift] key to highlight multiple items individually.

2. Either:
   - drag and drop the items to the Available Items column.
   - click the [Remove] button.

Applying changes to the selection list:

When you have finished updating the Selected Items list, click [Apply].

The Customize Selection pane is closed and the Selection list is updated to reflect your changes.

<table>
<thead>
<tr>
<th>Remove</th>
<th>Include Children</th>
<th>Type</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑️</td>
<td>☑️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>☑️</td>
<td>☑️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>☑️</td>
<td>☑️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>☑️</td>
<td>☑️</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Selecting List Items on Which to Perform a ControlPoint Operation

Some ControlPoint operations can be performed on individual items within a list or library. If the option to act on folders/items is available, a Choose link displays in the Include Children column for the list. (If you do not select individual folders/items, the operation will be performed on the list itself.)

NOTE For a multi-farm operation, you can only choose items from lists in the home farm. For lists in remote farms, the operation can only be performed on the list itself.
To include both the list itself and all of its child items:

In the Selection section, check the Include Children checkbox.

```
<table>
<thead>
<tr>
<th>Remove</th>
<th>Include Children</th>
<th>Type</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✗</td>
<td></td>
<td><a href="http://2010foundation/site/Documents/Forms/AllItem">http://2010foundation/site/Documents/Forms/AllItem</a></td>
</tr>
</tbody>
</table>
```

NOTE: The Include Children checkbox will not be visible if the operation requires that you select items explicitly. (Copy/Move List Items is a notable example).

To specify folders and items to include (with or without the list itself):

1. Click the Choose link to display the List Item picker.

   A pop-up window displays all of the items at the top level of the list hierarchy. If you want to display items within folders and subfolders, click the folder in the tree in the left pane. (You can drag the border between the left and right pane to resize, or click the arrow to open/close the left pane).
You can sort or filter list items by most of the column headers.

<table>
<thead>
<tr>
<th>Include Children</th>
<th>ID</th>
<th>Type</th>
<th>Name</th>
<th>Modified</th>
<th>Modified By</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>report</td>
<td>8/27/2009 5:30 PM</td>
<td>TestBench Acceler</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td></td>
<td>report2.csv</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If more than one view has been defined for a list or folder, you can select a different view from the Select view drop-down.

2 Use the information in the following table to determine the appropriate action(s) to take.

<table>
<thead>
<tr>
<th>If you want to include ...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>items with both inherited and non-inherited permissions</td>
<td>uncheck the Show items with unique permissions only box. &lt;br&gt;Note: If you leave this box checked, only items with unique (non-inherited) permissions will display.</td>
</tr>
<tr>
<td>all items and folders</td>
<td>check the box in the header. &lt;br&gt;Note: When you check this box and your selection includes folders, only the folder itself will be selected, not its children.</td>
</tr>
<tr>
<td>selected items and folders within the root of the list</td>
<td>check each item and folder that you want to include. &lt;br&gt;Note: If you check a box immediately to the left of a folder, only the folder itself will be selected, not its children.</td>
</tr>
<tr>
<td>all items within a folder</td>
<td>check the Include Children box to the left of the folder.</td>
</tr>
<tr>
<td>individual items within a folder</td>
<td>in the left pane: &lt;br&gt;· expand the folder, and &lt;br&gt;· select the item(s) you want to include.</td>
</tr>
</tbody>
</table>

Note: Normally, as you select items, the Total Selected Items value is updated automatically. Exceptions are if you check the box in the header to select all items then deselect items individually or if you select items by highlighting rows instead of explicitly clicking checkboxes. For both of these cases, you will need to click the Calculate Total link to update this value.

3 If, after you have finished selecting items you want to trim the list to display only selected items, check the Show All Selected Items box.

4 If you want to exclude the list itself (that is, perform the operation only on item(s) within the list, check the Remove Parent List from Selection box.
5 When you have finished, click [Apply].

Adding Objects from the SharePoint Hierarchy to Your Selection

After you have initiated a ControlPoint operation from the SharePoint Hierarchy, you can easily add objects to your selection using the Add to Selection menu option.

EXCEPTIONS:

You cannot add an object to your selection if the operation:

- has not yet been chosen from the menu
- is already within the scope of your selection (for example, you are attempting to add a site collection within a Web application that has already been selected)
- is not relevant for the object (for example, you initiated a Site Permissions analysis then attempted to add a list to your selection)
- can only be performed on a single object (such as a copy or move action).

NOTE: If you attempt to add an object to an operation that can only be performed on a single object, it will replace the object that was originally selected.

Saving and Re-Using a SharePoint Object Selection

If you frequently perform ControlPoint operations on the same set of SharePoint objects, you can save your selection to a local drive or network file share as an XML file. You can then upload the file on an as-needed basis, and eliminate the need to select the same set of objects whenever you perform a ControlPoint operation.

Only objects that are valid for the current operation will be included in the scope. For example:

- If your selection includes list items and you initiate an operation that is not valid for list items, those items will be excluded from scope.
• If you initiate an operation that can only be performed on a single object, the option to upload a selection from XML will not be available.

Generally, a selection saved on one farm cannot be uploaded to a different farm.

**EXCEPTION:** In a multi-farm environment, if a saved selection include items from more than one farm and you have initiated a ControlPoint operation that can act on multiple farms, it can be uploaded to any farm involved in the operation.

Once you have initiated an operation then upload a selection from XML, you have the option of replacing the current selection with the selection in the XML file or adding to it. It is important to note, however, that if you chose to *add* to the current selection and one group of objects is within the scope of the other (for example, the saved selection includes objects within the scope of the existing selection), the larger scope will be applied.

**To save a selection to an XML file:**

1. Initiate a ControlPoint operation for the selection you want to save.
2. In the Selection pane, click the **Save selection** link.

   ![Change selection](image)

   The Download File dialog displays.

   ![Download File - Windows](image)

3. Click **Download** to display the File Download dialog.
4. Click **Save** then save the file to the local or network location of your choice.

   **NOTE:** It is recommended that you change the default file name, Selection.XML, to a name that is unique and descriptive.
5 When the file has finished saving, click [Close] to dismiss the open dialogs.

**To upload a selection from an XML file:**

1 Initiate the ControlPoint operation you want to perform.
2 In the Selection section, click the **Upload Selection** link.

3 Click [Browse] and navigate to the file you want to upload.
4 The path to the file displays in the field to the left of the [Browse] button.
5 Click [Upload] to move the file path to the field below.
6 If you want the uploaded selection to **Replace Existing Selection**, check this box.

   **NOTE:** If you leave this box unchecked, the uploaded selection will be appended to the current selection.

7 Click [Apply].

**Selecting Users on Which to Perform a ControlPoint Action or Analysis**

When you initiate a ControlPoint action or analysis that involves SharePoint users, the Parameters section of the workspace includes the standard SharePoint "People Picker" for selecting the user(s) you want to include.
If you initiate an operation by selecting one or more users from the SharePoint Hierarchy, the People Picker will be pre-populated with the selected user(s).

You can:
- perform the operation on all SharePoint users (by leaving the People Picker blank)

OR

- select one or more individual users.

**Selecting Individual Users**

Enter the name of one or more users on which you want to perform the action or analysis. Separate each user name with a semicolon (;). Enter a full user account name (for example, `domain\username`), then click the Check Names icon (🛠) or press `[Ctrl] k` to validate the user name.

Depending on the action or analysis you are performing, ControlPoint may or may not allow invalidated users to be included in the operation. For example, you cannot add a user to a site unless the user’s existence in the provider database can be validated. However, you can **delete** or **report on** an unvalidated user’s permissions from a site, because it is reasonable to assume that a user who has been granted permissions to a SharePoint site may no longer exist in the provider database(s), as in the case of a terminated employee or a former customer.

**Operations that Include Two People Pickers**

When a ControlPoint action includes both a source and a target People Picker, such as Duplicate User Permissions, Delete User Permissions (when permissions are reassigned) and Migrate Users, additional rules and restrictions for user selection apply. Refer to the operation-specific topic in this guide for details.

**Refreshing the SharePoint Hierarchy**

Whenever you take an action that updates the SharePoint Hierarchy (such as adding or deleting a site, changing user permissions, and so on), you can immediately view changes in the SharePoint Hierarchy navigation tree by using the SharePoint Hierarchy menu option.
NOTE: This option is a faster, more efficient alternative to using the browser’s refresh button if you want to update only the SharePoint Hierarchy navigation tree rather than the entire page or active workspace. It is important to note, however, that when you refresh the SharePoint Hierarchy, the browser’s cache of previously-accessed items will be cleared (that is, the next time you access an item, ControlPoint will have to take the time to reload it).

To refresh the SharePoint Hierarchy:

In the SharePoint Hierarchy panel, right-click on the farm name and choose Refresh SharePoint Hierarchy.

In a multi-farm environment, each SharePoint Hierarchy is refreshed independently, from its own menu.

NOTE: When you refresh the SharePoint Hierarchy, any changes to ControlPoint menus will be viewable as well.

Reloading the Server-Side Hierarchy Cache

If the ControlPoint Application Administrator has configured ControlPoint to load site collections in the SharePoint Hierarchy from a server-side cache rather than in real-time, you can reload the server-side cache on an as-needed basis (for example, if a site collection has just been added or deleted) as follows:

From the Manage ControlPoint tree, choose ControlPoint Management > Reload Server-side Hierarchy Cache.

CAUTION: A reload of the server-side cache is a resource-intensive process that may affect application performance for all ControlPoint users.

This action will have no effect if the ControlPoint Configuration Setting PRELOADSITECACHE is set to false.

After reloading the server-side cache, you will need to refresh the SharePoint Hierarchy to clear the browser-side cache as well.
Searching for SharePoint Sites

The ControlPoint search functionality is designed to complement that used by native SharePoint.

The SharePoint search focuses on content (documents, users, and so on) based on metadata and/or words within the content. The ControlPoint search focuses on finding SharePoint sites based on their properties.

ControlPoint lets you:

- locate SharePoint sites by entering simple search terms or using an Advanced Search, and
- find a SharePoint site within the context of the ControlPoint SharePoint Hierarchy using the Search Hierarchy function.

A search can also be used to locate objects in the Change Selection pane and the various object pickers used throughout ControlPoint.

TIP: For locating sites within a very large farm, consider using the ControlPoint search functionality as a time-saving alternative to browsing through the SharePoint Hierarchy.

Performing a Simple or Advanced Search

To locate sites within your SharePoint environment, you can perform either:

- a simple search (by entering a full or partial site name or url), or
- an advanced search (by selecting from a variety of criteria on which to base your search).

NOTE: Simple and advanced searches use cached data collected by the Discovery job. This means that it will take less time to process than a hierarchy search, which uses real-time data. However, the search results will be as current as the time of the last Discovery run.
To perform a simple search:

1. From the left navigation frame choose Search.
2. Enter a full or partial site name in the Simple Search Terms box.
3. Click the magnifying glass icon (🔍).

NOTE: Results will include sites that match any part of the text string that you entered.

To perform an advanced search:

1. Use one of the following options:
From the SharePoint Hierarchy or Search Hierarchy results, select the object(s) on which you want to perform your search. Right-click and choose Advanced Search.

From the left navigation frame Search tab, choose Advanced Search.

NOTE: When you initiate your search from anywhere within the SharePoint Hierarchy, the scope of the search will be limited to sites within that level of the hierarchy. When you initiate the search from the Search tab, the search will include all matching sites within the farm.
2 In the Parameters section, select/enter the criteria you want to use to narrow your search.

Advanced Search  >  Select parameter(s) to act on

- Site Name contains
- Site URL contains
- Site Template Used or Not Used
- Web Parts Used or Not Used
- System Master Page Used or Not Used, and/or
- Site Theme Used or Not Used.

**NOTE:** Because the search uses cached data, the drop-down lists for the above attributes are populated with items that are current as of the last time Discovery was run and contain values that have actually been used within the selected scope.

- Security level that is currently in use in the site’s “has permissions” field.
- select whether you want to find sites which have permissions that are either Inherited or Unique.
• find sites for which a specific user has permissions; by selecting a user.

You can, optionally, further narrow your search by locating only those sites for which the user or group has permissions at a specific level.

If you have a SharePoint 2010 Server farm and the ControlPoint Application Administrator has defined Custom Properties, you can locate sites that have been assigned specific Custom Properties via the Set Site Properties action. (This section does not display for SharePoint 2007 or for 2010/2013 Foundation farms.)

NOTE: The search will return only those sites that meet all of the criteria you specify, including Not Used criteria. For example if you are searching for sites that do not use the Team Site template and do not use the Cardinal theme, only sites which use neither will be included in results.

All of the sites that meet the criteria you specified display in the Search Results.

If you want to initiate a new search or change search criteria, first click [Reset] to clear the contents of the Advanced Search window.

Working with Simple or Advanced Search Results

All simple and advanced search results pages include a standard header and footer, in addition to search results detail.
Search Results Toolbar

ControlPoint search results pages employ a report toolbar that contains page navigation, zoom, find, export, and print capabilities.

Search Results Header

The search results header sections contains summary information, including the search criteria used, as well as the scope of the search (as determined by the level at which the search was initiated).

The Cached field displays the date and time that the cache was last refreshed via the Discovery task. The search results are current as of that date and time.

Search Results Footer Information

The search footer contains the following information:

- the name of the administrator who generated the search (which can be useful if search results are exported or printed and distributed, since the content of the search reflects that administrator's permissions)
- the number of pages in the search (you can scroll through multi-page search results from the results toolbar in the search results header), and
- the date and time when the search results were generated.

Acting on Search Results

From search results you can perform any of the actions described in the following table.

<table>
<thead>
<tr>
<th>If you want to ...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>print search results</td>
<td>from the results toolbar:</td>
</tr>
<tr>
<td><strong>If you want to ...</strong></td>
<td><strong>Then ...</strong></td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>a) Click the Print Preview icon ( ).</td>
<td>A) Click the Print Preview icon ( ).</td>
</tr>
<tr>
<td>b) Click the print icon ( ).</td>
<td>B) Click the print icon ( ).</td>
</tr>
<tr>
<td>(Printed results will contain only the data that is currently expanded.)</td>
<td>(Printed results will contain only the data that is currently expanded.)</td>
</tr>
</tbody>
</table>

**export search results**

<table>
<thead>
<tr>
<th><strong>Then ...</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>choose an <strong>Export to the selected format</strong> option from the drop-down, then click the <strong>Export</strong> link.</td>
</tr>
</tbody>
</table>

**NOTE:** If you export to Excel, all data will be exported, regardless of whether it is expanded. If you export to an Acrobat (PDF) file, only data that is currently expanded will be exported.

**download raw analysis result data to a CSV file that can be imported into another program for further examination**

<table>
<thead>
<tr>
<th><strong>Then ...</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>click the <strong>Download Report Data as CSV</strong> hyperlink in the results toolbar.</td>
</tr>
</tbody>
</table>

This option differs from the csv option in the Export... drop-down in that it provides all of the raw data (including object GUIDs and internal field names, for example) used to create the results. This may be useful for troubleshooting or for more in-depth analysis.

**perform a ControlPoint action or analysis within the current workspace**

<table>
<thead>
<tr>
<th><strong>Then ...</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>use the procedure for <strong>Acting on Search or Data Analysis Results</strong>.</td>
</tr>
</tbody>
</table>

---

**Searching within the SharePoint Hierarchy**

Use the Search Hierarchy feature to locate sites within the ControlPoint SharePoint Hierarchy.

This feature is a useful alternative to the SharePoint Hierarchy for navigating through a large farm.

You can initiate a SharePoint Hierarchy search from various locations in the SharePoint Hierarchy panel, as well as from the Search Hierarchy panel. The scope of the search is determined by the location in the hierarchy from which it was initiated. That is, if you initiate the search at the farm level or directly from the Search Hierarchy menu, all matching sites within the farm will display. If you initiate the search at the Web application level, results will be limited to matching sites within the Web application, and so on. In a multi-farm environment, you can only search the home farm.

**NOTE:** By default, the Search Hierarchy feature uses real-time data. However, to enable faster
searches in large environments, ControlPoint Application Administrators can configure the application to use cached data for hierarchical searches.

**To perform a hierarchy search:**

1. Use the information in the table below to determine the appropriate action to take.

<table>
<thead>
<tr>
<th>If you want to initiate your search from ...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>within the SharePoint Hierarchy panel</td>
<td>from the appropriate level of the hierarchy, right-click and choose Search Hierarchy.</td>
</tr>
<tr>
<td>the Search Hierarchy panel</td>
<td>From the left navigation header, choose Search.</td>
</tr>
</tbody>
</table>

2. Enter a full or partial **Name** and/or **URL**.

3. Click the magnifying glass icon (🔍).
   
   All of the sites and subsites that meet all of your search criteria display—along with associated lists, users and groups—within the appropriate hierarchical context,
   
   You can navigate through search results and access SharePoint pages and ControlPoint actions and analyses via the right-click menu.
Managing SharePoint Objects

From the SharePoint Hierarchy panel, you can access a variety of SharePoint administration pages and ControlPoint value-added actions for managing SharePoint objects.

Accessing SharePoint Pages

From the SharePoint Hierarchy panel, you can

- access the relevant SharePoint administration page for managing a SharePoint object, and
- open a SharePoint site or list.

One of the advantages of using ControlPoint over native SharePoint to access these pages is that you can link directly to the appropriate page, within the relevant context, and without having to enter a url. In a multi-farm environment, you can access SharePoint pages for either the home farm or a remote farm.

Consult your SharePoint documentation for information on using SharePoint administration features to manage SharePoint objects.

Accessing SharePoint Site Collection Administration Pages

From a site collection's right click menu, you can access a variety of SharePoint pages for managing the site collection, including

- Site Settings (for the root site)
- Configuration pages for operations that include setting site properties such as quotas and administrators.

- Pages for managing a site collection's content, including Content and Structure and site creation and site collection deletion.
Accessing SharePoint Site Administration Pages

From a site's right click menu, you can access a variety of SharePoint pages for managing the site, including:

- Site Settings

- options for managing site Content including creating and deleting subsites
• options for managing Users and Security, including users, groups, and permissions for the site.

Opening a SharePoint Site in ControlPoint

From the SharePoint Hierarchy panel, you can open a SharePoint site or list in the ControlPoint workspace pane.
To open a SharePoint site in ControlPoint:

From the site's right-click menu, choose Open Site.

Accessing SharePoint Pages for Managing Libraries and Lists

The Lists folder contains all of the libraries and lists currently used in a site.

NOTE: Three asterisks (*** ) to the left of a list name indicates that the list has unique (non-inherited) permissions.

You can link directly to the SharePoint pages for managing the settings of an existing list or open a list.

NOTE: If the Lists folder does not display for a selected site, libraries or lists have not yet been created.

Deleting Sites

The ControlPoint Delete Sites action lets you delete one or more sites from your SharePoint farm.
If you delete an entire site collection (by deleting its root site) from the source content database, any activity associated with it remains but becomes "orphaned." The site collection in the source content database will display as a deleted site collection in Site Collection Activity results only if it was active during the period covered by the analysis. A deleted site will continue to be included in activity and storage analysis results if it was active during the period covered by the analysis.

To delete one or more sites from your SharePoint farm:

1. Select the site(s) that you want to delete.
   NOTE: If you want to delete an entire site collection—and have permissions to do so—select the root site (which, by extension, includes all of its subsites).

2. Choose Content > Delete Site.

Now you can either:

- run the operation immediately (by clicking the [Run Now] button)

OR

- schedule the operation to run at a later time.

OR

- save the operation as XML Instructions that can be executed at a later time.

If you chose the Run Now option, after the action has been processed:

- a confirmation message displays at the top of the page, and
- a ControlPoint Task Audit is generated for the action and displays in the Results section.

If you schedule the action, a link to the Task Audit is included in the scheduled action notification email.

See also Auditing ControlPoint Administrator Tasks.

Deleting Lists

The ControlPoint Delete Lists action lets you delete one or more sites from your SharePoint farm in real time.

To delete one or more lists from your SharePoint farm:

1. Select the list(s) that you want to delete.

2. Choose Content > Delete List.

Now you can either:

- run the operation immediately (by clicking the [Run Now] button)
OR

- schedule the operation to run at a later time.

OR

- save the operation as XML Instructions that can be executed at a later time.

If you chose the Run Now, option, after the action has been processed:

- a confirmation message displays at the top of the page, and
- a ControlPoint Task Audit is generated for the action and displays in the Results section.

If you schedule the action, a link to the Task Audit is included in the scheduled action notification email.

See also Auditing ControlPoint Administrator Tasks.
Managing Metadata

ControlPoint offers two actions for managing metadata created via the SharePoint Online Term Store Management Tool:

- **Set Metadata Value** lets you change Managed Metadata, text, or numeric value values for one or more lists or libraries.
- **Create Managed Metadata** lets you create or update a Managed Metadata column on a list or library from an existing text column.

You can also **analyze Managed Metadata usage within your SharePoint Server environment**.

It is assumed that, when using these features, you are familiar with the use and behavior of SharePoint Content Types and Managed Metadata.

Setting Metadata Values

ControlPoint lets you populate or change Managed Metadata, a single line of text, or numeric values within a list column for a selected Content Type.

You can also run a simulation of how the operation will be carried out before committing to the action. This can be valuable, for example, to identify exactly which items would be changed.

EXAMPLE:

The Shared Documents library on the company website has a Managed Metadata column called **Location**.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Modified</th>
<th>Modified By</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>![ ]</td>
<td>Davinci Component Diagram</td>
<td>9/20/2011 6:13 PM</td>
<td>install</td>
<td>Middletown</td>
</tr>
<tr>
<td>![ ]</td>
<td>Help Topic IDs</td>
<td>9/15/2011 5:19 PM</td>
<td>System Account</td>
<td></td>
</tr>
<tr>
<td>![ ]</td>
<td>LabManual</td>
<td>9/15/2011 5:19 PM</td>
<td>System Account</td>
<td></td>
</tr>
</tbody>
</table>

Add document
I want to make sure that the value Woburn is added to the Location column for all documents in that library.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Modified</th>
<th>Modified By</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Addendum</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Davinci Component Diagram</td>
<td>9/20/2011 6:54 PM</td>
<td>System Account</td>
<td>Middletown; Boston</td>
</tr>
<tr>
<td></td>
<td>Help Topic IDs</td>
<td>9/20/2011 6:54 PM</td>
<td>System Account</td>
<td>Boston</td>
</tr>
<tr>
<td></td>
<td>LabManual</td>
<td>9/20/2011 6:54 PM</td>
<td>System Account</td>
<td>Boston</td>
</tr>
<tr>
<td></td>
<td>Managing SharePoint Security</td>
<td>9/20/2011 6:54 PM</td>
<td>System Account</td>
<td>Los Angeles; Boston</td>
</tr>
</tbody>
</table>

**To set a metadata value:**

1. Select the object(s) whose column data you want to set.
2. Choose Automation > Set Metadata Value.

   Set Metadata Value > Select parameter(s) to act on

   ![Select a Column Type](Select a Column Type: Managed Metadata, Text, Numeric)

   ![Select a Column](Select a Column: Content Type Contains, Get Content Types (takes more time), Content Type, Column)

   ![Choose a Value](Choose a Value: New Value, Please type here..., Overwrite existing values, Append to existing values)

3. Select the type of metadata you want to set:
   - Managed Metadata
   - Single Line Text, or
   - Numeric
4 Use the information in the following table to determine the appropriate action to take.

<table>
<thead>
<tr>
<th>If the scope of your selection ...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>• is at the site level or above and/or • includes more than one list</td>
<td>go to the next step. NOTE: Before you can select a list column, you must first choose from available Content Types.</td>
</tr>
<tr>
<td>consists of only one list</td>
<td>you may want to go to Step 8. NOTE: It is not necessary to choose a Content Type for a single list. The Column drop-down will automatically populate with all of the columns used by that list.</td>
</tr>
</tbody>
</table>

5 If you want to filter content types by a specific text string, complete the Content Type Contains field.

   Select a Source Text Column

   Content Type Contains: doc

6 To populate the Content Type drop-down with relevant Content Types, click [Get Content Types].

7 Select a Content Type from the drop-down.

8 Select the Column whose value you want to set. (This drop-down is populated with all of the columns used by lists within the scope of your selection that match the selected data type and content type.)

   NOTE: If your selection includes more than one list, custom columns will only appear in the drop-down if they have been added to the Content Type at the site level. If a column was added directly to a particular list (or to a Content Type on the list), it will appear in the drop-down if your selection consists of only that list.

9 For Choose a Value:

   a) Enter the new value for the column (For Managed Metadata, you can also click the icon and select from available values.)
b) If you want to **overwrite existing values**, check this box.

   **NOTE:** If you leave this box unchecked and a value already exists in that column for an item, it will be skipped. If you selected a Managed Metadata column that allows multiple values, you also have the option to **append to existing values**.

Now you can either:

- run a simulation of the action (by clicking [Run Simulation])
- run the action immediately (by clicking [Run Now]),

**OR**

- schedule the action to run at a later time.

**OR**

- create an xml file with instructions for the analysis that can be executed at a later time (by clicking [Save Instructions]).

If you click [Run Simulation], ControlPoint runs through the process without actually making changes. A Task Audit will be generated with a description of what ControlPoint *would have done* if the action had been carried out. Text in the task description identifies it as a simulation.

If you chose the Run Now, option, after the action has been processed:

- a confirmation message displays at the top of the page, and
- a ControlPoint Task Audit is generated for the action and displays in the Results section.

If you schedule the action, a link to the Task Audit is included in the scheduled action notification email.

See also [Auditing ControlPoint Administrator Tasks](#).

---

**Creating a Managed Metadata Column from a Text Column (SharePoint Server)**

The Create Managed Metadata action lets you map an existing text column in a SharePoint list or library to a Managed Metadata term. You can:

- map the text column to a Managed Metadata column that is already used by the list/library

**OR**

- create a new Managed Metadata column using a term set that has been defined either within the current site collection or in the Managed Metadata Service Application.
NOTE: If ControlPoint creates the Managed Metadata column, it will do so on the list-level Content Type. If you have defined a Content type at a higher level (such as the site collection or site) you may want to manually update the shared definition, and then use this action to populated the values of that column.

You can also run a simulation of how the operation will be carried out before committing to the action. This can be valuable, for example, to identify exactly which items would be changed.

EXAMPLE:

A SharePoint document library has a text field called Office, which identifies the Metalogix regional office that has ownership of a document.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Modified</th>
<th>Office</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ControlPoint User Guide Addendum</td>
<td>9/21/2011 11:03 AM</td>
<td>Woburn</td>
</tr>
<tr>
<td></td>
<td>Davinci Component Diagram</td>
<td>9/21/2011 11:04 AM</td>
<td>East Podunk</td>
</tr>
<tr>
<td></td>
<td>Help Topic IDs</td>
<td>9/21/2011 10:30 AM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Managing SharePoint Security</td>
<td>9/21/2011 11:04 AM</td>
<td>Los Angeles</td>
</tr>
</tbody>
</table>

The SharePoint administrator wants to map that column to a new Managed Metadata column entitled Metalogix Office, populate the new column with only valid Managed Metadata, and rename the original column, which is retained for reference or cleanup.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Modified</th>
<th>Obsolete</th>
<th>Metalogix Office</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Davinci Component Diagram</td>
<td>9/21/2011 2:41 PM</td>
<td>East Podunk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Help Topic IDs</td>
<td>9/21/2011 2:33 PM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To create Managed Metadata from a text column:

1. Select the object(s) for which you want to create Managed Metadata.
2. Choose Automation > Create Managed Metadata.

Create Managed Metadata > Select parameter(s) to act on 🔄

<table>
<thead>
<tr>
<th>Select a Source Text Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Type Contains:</td>
</tr>
<tr>
<td>Content Type:</td>
</tr>
<tr>
<td>Source Column Name:</td>
</tr>
<tr>
<td>Update source column to:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Select a Target Managed Metadata Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Column Name:</td>
</tr>
<tr>
<td>Description:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Require that this column contains information</td>
</tr>
<tr>
<td>Enforce unique values</td>
</tr>
<tr>
<td>Add to all content types</td>
</tr>
<tr>
<td>Add to default view</td>
</tr>
<tr>
<td>Display format:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Select term (Default value):</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Target Column Options</td>
</tr>
<tr>
<td>------------------------</td>
</tr>
<tr>
<td>If source value does not match term:</td>
</tr>
<tr>
<td>Leave target column as is</td>
</tr>
<tr>
<td>Use Blank in target column</td>
</tr>
<tr>
<td>Use Default value (term) in target column</td>
</tr>
</tbody>
</table>

3. Use the information in the following table to determine the appropriate action to take.

<table>
<thead>
<tr>
<th>If the scope of your selection ...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>is at the site level or above</td>
<td>go to the next step.</td>
</tr>
</tbody>
</table>
and/or
• includes more than one list

NOTE: Before you can select a list column, you must first choose from available Content Types.

consists of only one list

you may go to Step 7.

NOTE: It is not necessary to choose a Content Type for a single list. The Column drop-down will automatically populate with all of the columns used by that list.

4 If you want to filter source column content types by a specific text string, complete the Content Type Contains field.

| Select a Source Text Column |
|-----------------------------|-----------------------------|
| Content Type Contains: doc | X                           |

5 To populate the Content Type drop-down with relevant content types, click [Get Content Types].

6 Select a source column Content Type from the drop-down.

NOTE: If you have selected objects above the list level (for example, Web applications, site collections, and/or sites), the drop-down will be populated with all Content Types that are available for use by lists and libraries within the scope of your selection. If you have selected multiple lists, only Content Types that are currently in use by those lists will be available for selection.
Select the **Source Column Name** of the column whose value you want to use in setting the Managed Metadata field. (This drop-down is populated with all of the *text* columns within the scope of your selection that match the selected Content Type.)

NOTE: If your selection includes more than one list, custom columns will only appear in the drop-down if they have been added to the Content Type at the site level. If a column was added directly to a particular list (or to a Content Type on the list), it will appear in the drop-down if your selection consists of only that list.

If you want to give the source column a new name, complete the **Rename source column to** field. (If you want to use the same name for the target column, then you must rename the source column.)

Complete the **Select a Target Managed Metadata section** as follows:

a) For **Target Column Name** and **Description**:

   - If the Managed Metadata column already exists for the Content Type, select it from the drop-down.

   **NOTE:** When you select an existing Managed Metadata column, the remaining fields will be grayed-out, and the existing column definition will be used.

   OR

   - If you want to create a Managed Metadata column for the Content Type, enter a name for the new column in the drop-down then enter a **Description**.

   **NOTE:** If you are creating a new Managed Metadata column, complete the remaining fields as you would if you were creating it in SharePoint.

10 Check the options that you want to apply to the target column.
11. Complete the **Target Column Options** section as follows:

   a) For **If source value does not match term**, specify how to proceed if a source value does not match a valid term within the selected term set. Use the information in the following table for guidance.

   ![Target Column Options Table]

<table>
<thead>
<tr>
<th>If source value does not match term</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leave target column as is</td>
<td>select <em>Leave target column as is.</em></td>
</tr>
<tr>
<td>Use Blank in target column</td>
<td>select <em>Use Blank in target column.</em></td>
</tr>
<tr>
<td>Use Default value (term) in target column</td>
<td>select <em>Use Default value (term) in target column.</em></td>
</tr>
<tr>
<td>Overwrite existing values</td>
<td></td>
</tr>
<tr>
<td>Append to existing values</td>
<td></td>
</tr>
</tbody>
</table>

   b) If the target Managed Metadata column already exists and you want to **Overwrite existing values**, check this box.

   **NOTE:** If you leave this box unchecked and a value already exists in that column for an item, the existing value will be retained. If you selected a Managed Metadata column that allows multiple values, you also have the option to **Append to existing values**.

Now you can either:

- run a simulation of the action (by clicking [*Run Simulation]*)
- run the action immediately (by clicking [*Run Now*]),

OR
• **schedule the action to run at a later time**

OR

• **create an xml file with instructions for the analysis that can be executed at a later time** (by clicking [Save Instructions]).

If you click [Run Simulation], ControlPoint runs through the process without actually making changes. A Task Audit will be generated with a description of what ControlPoint *would have done* if the action had been carried out. Text in the task description identifies it as a simulation.

If you chose the Run Now, option, after the action has been processed:

• a confirmation message displays at the top of the page, and
• a ControlPoint Task Audit is generated for the action and displays in the Results section.

If you schedule the action, a link to the Task Audit is included in the scheduled action notification email.

See also [Auditing ControlPoint Administrator Tasks].
Managing SharePoint User Permissions

ControlPoint includes a variety of value-added actions that facilitate the management of SharePoint users, groups, and permissions:

These actions are accessible from various levels of the hierarchy, enabling you to act on a single site collection or site, multiple site collections, sites, and/or lists within a Web application, or across the entire farm.

EXCEPTION: You cannot use these actions to manage user permissions for the SharePoint Central Administration site.

From the ControlPoint left navigation pane, you can also link directly to SharePoint pages for managing users and permissions.

Accessing SharePoint Pages for Managing User Permissions

The Users folder displays all of the users with direct or explicit permissions for a selected site collection or site. You can link directly to the SharePoint pages for managing direct permissions of an existing user or create a new user.

NOTE: Users do not display for sites whose permissions are inherited (as indicated by a site icon).

If a user has permissions to the site collection/site via a group, permissions are managed at the group level. See Accessing SharePoint Pages for Managing Groups.
To view user permissions for the site collection/site in SharePoint

Click on the Users folder to access the SharePoint Permissions page for the site collection/site.

To view/edit information about a user in SharePoint:

Select a user name and choose Edit to access the SharePoint Edit Personal Settings page for that user.
As an alternative to managing permissions through SharePoint, you can use ControlPoint value-added features for managing user permissions. These features are especially useful if you want act on multiple users and/or across multiple sites in a single operation.

**Accessing SharePoint Pages for Managing Groups**

The Groups folder displays all of the SharePoint and Active Directory groups with permissions for a site. You can link directly to the SharePoint pages for managing an existing group or create a new group.

All groups with permissions for each site within a site collection display beneath the site. In the case of SharePoint groups, the number of users within a group, as well as the group’s permission level, displays to the right of each group name.

NOTE: Groups do not display for sites whose permissions are inherited (as indicated by the icon).

You can view group membership by clicking on the plus sign (+) to the left of the group name.
To view/edit an existing group in SharePoint:

Click on a SharePoint group name to access the SharePoint People and Groups page for that group.

To view/edit groups in SharePoint:

Click the Groups folder to access the SharePoint All Groups page, from which you can create a new group for the site.
Consult your SharePoint documentation for instructions on creating a group.

NOTE: If the Groups folder does not display for a root site or a site with unique permissions, no groups have been granted permissions for it. To set up permissions for the first Group, navigate to the People and Groups page through the SharePoint site. Once a group has been granted permissions, the Groups folder will display in the ControlPoint left navigation pane as soon as you refresh the SharePoint Hierarchy.

### Setting User Direct Permissions

Set User Direct Permissions is a ControlPoint action that lets you grant users direct permissions to one or more SharePoint sites, lists/libraries, and/or items. (The action will not, however, overwrite or replace any direct permissions a user may already have.)

NOTE: If you want to add users to an existing SharePoint group, use the procedure for Adding Users to SharePoint Groups.

To set user direct permissions:

1. Select the object(s) to which you want to grant user permissions.
2. Choose Users and Security > Set User Direct Permissions.
3 Complete the Parameters section as follows:

a) For **Set Permissions for User(s)**, select the user(s) for whom you want to set direct permissions.

b) In the **Permission Level (Direct)** drop-down, select a level from the list.

![Permission Levels dropdown]

NOTE: All custom permissions levels that are currently assigned to at least one user within the scope of your selection display in the drop-down. (In a multi-farm environment, this list is populated from the permissions of the home farm.) If you want to assign a custom permissions level that has been defined for a site collection but either is not currently in use or exists only on a remote farm, you can type it into the drop-down.

c) If your selection includes one or more sites and you want the permissions to be applied to all lists within the site(s) that have unique permissions, check the **Propagate to All Lists with Unique Permissions** box.

d) If you have checked the **Propagate to All Lists with Unique Permissions** box and want the permissions to be applied to all items within the list(s) that have unique permissions, check the **Propagate to List Items** box.

NOTE: The "Propagate" options do not apply to lists that you selected explicitly. If you want to include items within explicitly-selected lists, use the **Include Children** or **Choose** option in the Selection panel. See also [Selecting List Items on Which to Perform a ControlPoint Operation](#).

Now you can either:

- run the operation immediately (by clicking the **[Run Now]** button)

OR

- **schedule the operation to run at a later time**.

OR

- **save the operation as XML Instructions that can be executed at a later time**.

If you chose the Run Now option, after the operation has been processed:

- a confirmation message displays at the top of the page, and

- a ControlPoint Task Audit is generated for the operation and displays in the Results section.

If you schedule the operation, a link to the Task Audit is included in the scheduled action notification.
email.

See also Auditing ControlPoint Administrator Tasks.

Deleting User Permissions

Delete User Permissions is a ControlPoint action that lets you delete SharePoint user permissions from one or more site collections/sites. You can also choose whether to:

- delete the user’s entry from the selected site(s) (so that they no longer appear in the site’s All People list)
- delete alerts associated with the user
- delete the user’s My Site site collection, and/or
- reassign a user’s permissions to one or more target users before performing the deletion

EXCEPTION: You cannot reassign Site Collection Administrator privileges using this action.

CAUTION: Deleting Users from SharePoint Groups

The Delete User Permissions action will remove the selected user(s) from SharePoint groups in which they are listed as a member. Because groups are defined at the site collection level and may be used anywhere in the site collection, if you are performing the action on one or more individual sites that includes groups that are used elsewhere in the site collection, the user(s) will lose permissions on unselected sites within the collection as well.

NOTE: This action does not remove users from Active Directory groups. Therefore, if a user is granted permissions via an Active Directory group, those permissions will not be impacted.

Deleting Permissions from Lists, Folders, or Items with Unique Permissions

When user permissions are added to a list, folder, or item that has unique permissions, SharePoint automatically creates an entry for the user on its first non-inherited parent object and assigns a permissions level of “Limited.” This entry will be deleted only if that parent object is included in the scope of the action. If the parent object is not included in the scope, the following message will display in the Task Audit:

User [user_name] permissions cannot be removed from [object_type] [object_name]. Go to the first non-inheriting parent [object_type] to remove this permission.

To delete the permissions of one or more users:

1. Select the object(s) from which you want to delete permissions.
2. Choose Users and Security > Delete User Permissions.
3. For Delete All Permissions for User(s), select the user whose permissions you want to delete.
NOTE: Delete User Permissions is one of the ControlPoint actions that can be performed on unvalidated users. (For example, you can delete the SharePoint permissions of a user that you know has been removed from Active Directory or alternate authentication provider database.) However, any individual user(s) entered into the Reassign Deleted Permissions to People Picker must be validated.

4 Specify the remaining parameters as appropriate. Use the information in the table below for guidance.

<table>
<thead>
<tr>
<th>If you want to ...</th>
<th>Then ...</th>
</tr>
</thead>
</table>
| remove the user(s) from the site collection's People and Group list | check the **Delete User Entries from the Site Collection** box . (If you leave this box unchecked, permissions will be deleted but user entries will remain in the People and Groups list). NOTES:  
  - If a user was granted permissions *only* through an Active Directory group, that user may have an “invisible entry” in the site collection’s People and Group list. This action will remove that entry.  
  - If the **Delete direct permissions only** is selected, this option becomes disabled. The removal of a user from the site collection would remove *all* of that user’s permissions, including those granted through membership in SharePoint groups.  |
| remove only direct permissions and retain permissions granted through SharePoint group membership | check the **Delete direct permissions only (Leave group permissions intact)** box.  
  NOTE: If **Delete User Entries from the Site Collection is selected**, this option becomes disabled. Removal of a user from the site collection would remove *all* of that user’s permissions, including those granted through membership in SharePoint groups.  |
| reassign the permissions of the user(s) to be deleted to one or more other users | a. Check the **Reassign Deleted Permissions to** box. b. Select the user(s) to whom you want to copy the permissions.  
  ![Reassign Deleted Permissions to:](image)  
  **James Joyce** ;  
  NOTE: If you entered the name of more than one user in the Delete Users field, the permissions of every one of those users (if different) will be reassigned to the target user.  |
Now you can either:

- run the operation immediately (by clicking the [Run Now] button)

OR

- schedule the operation to run at a later time.

OR

- save the operation as XML Instructions that can be executed at a later time.

If you chose the Run Now, option, after the operation has been processed:

- a confirmation message displays at the top of the page, and

- a ControlPoint Task Audit is generated for the operation and displays in the Results section.

If you schedule the operation, a link to the Task Audit is included in the scheduled action notification email.

See also Auditing ControlPoint Administrator Tasks.

NOTE: If you chose to reassign permissions, the delete action will not be carried out unless the permissions are successfully reassigned.

Duplicating a User's Permissions

Duplicate User Permissions is a ControlPoint action that lets you copy the permissions of one SharePoint user to one or more others. Permissions can be copied for multiple site collections in a farm or Web application, or for individual site collections and sites.

EXCEPTIONS: You cannot duplicate Site Collection Administrator privileges using this action. You also cannot duplicate permissions that were granted via an Active Directory group (as an alternative, you can simply add the new user(s) to the Active Directory group).

All of a user's permissions for a site collection, including any unique permissions for sites, lists, and libraries, and items are copied.

NOTE: If your ultimate goal is to delete a user after copying his or her permissions to another user (for example, if the user is leaving the department or company and is being replaced by someone else), you can do so as part of the procedure for Deleting User Permissions.

To duplicate a user's permissions:

1. Select the site(s) for which you want to duplicate permissions.
2 Choose Users and Security > Duplicate User Permissions.

3 Complete the Parameters section as follows:

   a) For **Model User Name**, select the user(s) whose permissions you want to duplicate.

   NOTE: Make sure that the permissions of the user you want to use as the model are appropriate for the target user(s). Remember that you can review the permissions of the model before continuing. If you entered the name of more than model user, the permissions of every one of those users (if different) will be assigned to the target user(s).

   b) For **Duplicate Permissions To**, select the target user(s).

   c) If you want permissions of the model user(s) to replace those of the target user(s), check the **Delete existing permissions from target** box.

   NOTE: If you leave this box unchecked, model user permissions will be added to any existing permissions.

Now you can either:

- run the operation immediately (by clicking the [Run Now] button)

OR

- **schedule the operation to run at a later time.**

OR

- **save the operation as XML Instructions that can be executed at a later time.**

If you chose the Run Now, option, after the operation has been processed:

- a confirmation message displays at the top of the page, and
- a ControlPoint Task Audit is generated for the operation and displays in the Results section.

If you schedule the operation, a link to the Task Audit is included in the scheduled action notification email.

See also **Auditing ControlPoint Administrator Tasks.**

### Adding Users to SharePoint Groups

Add Users to SharePoint Groups is a ControlPoint action that enables you to add one or more users to existing SharePoint groups.

**To add users to SharePoint groups:**

1. **Select the object(s) for which you want to add users to groups.**
2. Choose Users and Security > Add User to SharePoint Group.
3 Select the SharePoint group(s) to which you want to add users as follows:
   a) From the Available Items list, select the group(s) to which you want users and move them to the Selected Items list.
      Note that all groups defined for the entire site collection display beneath the root site. Groups with unique permissions also display beneath the site granting those permissions. By default, groups will display in this list if they have been assigned at least one permissions level. ControlPoint Application Administrators can, however, configure ControlPoint to display groups that do not have an associated permissions level. Details can be found in the ControlPoint Administration Guide.
   b) When you have finished adding groups to the Selected Items list, click [Apply].

4 In the Parameters section Choose User(s) field, select the user(s) that you want to add to the group(s).

5 If you want to remove any user direct permissions from objects for which the selected group has permissions, check the Remove matching direct permissions box.

   NOTE: Direct permissions for any objects within the scope of the action for which the selected SharePoint group does not have permissions will be retained.

Now you can either:
• run the operation immediately (by clicking the [Run Now] button)

OR

• schedule the operation to run at a later time.

OR

• save the operation as XML Instructions that can be executed at a later time.

If you chose the Run Now, option, after the operation has been processed:

• a confirmation message displays at the top of the page, and

• a ControlPoint Task Audit is generated for the operation and displays in the Results section.

If you schedule the operation, a link to the Task Audit is included in the scheduled action notification email.

See also Auditing ControlPoint Administrator Tasks.

Setting SharePoint Group Permissions

The Set SharePoint Group Permissions action lets you assign a permissions level to one or more SharePoint groups within a single site collection or site.

By default, only groups that have existing permissions within the site collection can be selected. In that case, the action adds to the existing permissions (it does not replace them). ControlPoint Application Administrators can, however, choose to display? and allow the selection of? groups that exist in the site collection but do not have permissions to the object. See the ControlPoint Administration Guide for details on changing the ControlPoint Setting “Show SharePoint Groups with No Permissions in Hierarchy.”

In a multi-farm environment, SharePoint group permissions can be set on a single farm; either the home farm or a remote farm.

**To set SharePoint Group Permissions**

1. Select the site collection or site whose SharePoint group permissions you want to set.
2 Choose Users and Security > Set SharePoint Group Permissions.

Select SharePoint Groups:

Control-click to select multiple items from the left side. Right-click for additional options.

Available Items

Group: [ ] Show Orphans
Name: 
URL:

Beta Aquatics (25)
Beta Aquatics - Root Site
Alpha Snackfoods Owners [None] (1)
Beta Aquatics Owners [Full Control] (2)
Beta Aquatics Visitors [Read] (2)
Marketing Team [Design] (2)
Policy Test Group [Policy Test] (2)
Sales Team [Contribute] (4)
Viewers [View Only]

Selected Items

SharePoint - 00
Beta Aquatics
Beta Aquatics - Root Site
Alpha Snackfoods Owners [None] (1)

Select & Drag
Add >
< Remove
Select & Drag

3 Select the group(s) to which you want to add permissions as follows:

a) From the Available Items list, select the group(s) to which you want to set permissions and move them to the Selected Items list.

Note that all groups defined for the entire site collection that have at least one associated permissions level display beneath the root site. Groups with unique permissions also display beneath the site granting those permissions. Any group that does not have at least one associated permissions level for the site collection or site will not display in the list.

TIP: If your Available Items list is particularly long, you may find it useful to narrow the scope by searching based on Group name, site Name, and/or site URL) and searching for the group. For example, if you want to narrow your scope to all group owners, enter "owner" in the Group field.

b) Click [Apply].

4 From the Permission Level drop-down, select the permissions level you want to add to the group.
REMINDER: This action will add to, but will not replace, an existing permissions level.

Select SharePoint Groups:

Control-click to select multiple items from the left side. Right-click for additional options.

NOTE: All custom permissions levels that are currently assigned to at least one user within the scope of your selection display in the drop-down. (In a multi-farm environment, this list is populated from the permissions of the home farm.) If you want to assign a custom permissions level that has been defined for a site collection but either is not currently in use or exists only on a remote farm, you can type it into the drop-down.

5 If your selection includes one or more sites and you want the permissions to be applied to all lists within the site(s) that have unique permissions, check the Propagate to All Lists with Unique Permissions box.

6 If you have checked the Propagate to All Lists with Unique Permissions box and want the permissions to be applied to all items within the list(s) that have unique permissions, check the Propagate to List Items box.

NOTE: The "Propagate" options do not apply to lists that you selected explicitly. If you want to include items within explicitly-selected lists, use the Include Children or Choose option in the Selection panel. See also Selecting List Items on Which to Perform a ControlPoint Operation.

Now you can either:

- run the operation immediately (by clicking the [Run Now] button)

OR

- complete the Enforce Policy section and schedule the operation to run at a later time.

OR

- save the operation as XML Instructions that can be executed at a later time.
Deleting SharePoint Group Permissions

The Delete SharePoint Group Permissions lets you delete the permissions of one or more SharePoint groups from a single site collection or site without removing its members or deleting the group itself.

NOTE: This action deletes all permissions currently assigned to a group. Once permissions have been removed from a SharePoint group, the group will display in the SharePoint Group Analysis. Whether or not the group continues to display in the SharePoint Hierarchy or any ControlPoint group pickers depends on the Parameter Value of the ControlPoint Configuration Setting ShowNoPermSPGroup.

To delete SharePoint Group Permissions:

1. Select the site collection or site whose group permissions you want to delete.
2. Choose Users and Security > Delete SharePoint Group Permissions.
3. Select the group(s) whose permissions you want to delete as follows:
   a) From the Available Items list, select the group(s) to which you want to add users and move them to the Selected Items list.
      Note that all groups defined for the entire site collection that have at least one associated permissions level display beneath the root site. Groups with unique permissions also display
beneath the site granting those permissions. Any group that does not have at least one associated permissions level for the site collection or site will not display in the list.

TIP: If your Available Items list is particularly long, you may find it useful to narrow the scope by searching based on Group name, site Name, and/or site URL) and searching for the group. For example, if you want to narrow your scope to all group owners, enter "owner" in the Group field.

b) Click [Apply].

4 If your selection includes one or more sites and you want the permissions to be deleted from all lists within the site(s) that have unique permissions, check the Propagate to All Lists with Unique Permissions box.

5 If you have checked the Propagate to All Lists with Unique Permissions box and want the permissions to be deleted from all items within the list(s) that have unique permissions, check the Propagate to List Items box.

NOTE: The "Propagate" options do not apply to lists that you selected explicitly. If you want to include items within explicitly-selected lists, use the Include Children or Choose option in the Selection panel. See also Selecting List Items on Which to Perform a ControlPoint Operation.

Now you can either:

- run the operation immediately (by clicking the [Run Now] button)

OR

- complete the Enforce Policy section and schedule the operation to run at a later time.

OR

- save the operation as XML Instructions that can be executed at a later time.

If you chose the Run Now, option, after the operation has been processed:

- a confirmation message displays at the top of the page, and
- a ControlPoint Task Audit is generated for the operation and displays in the Results section.

If you schedule the operation, a link to the Task Audit is included in the scheduled action notification email.

See also Auditing ControlPoint Administrator Tasks.

Deleting SharePoint Groups

Use the Delete SharePoint Groups action to delete SharePoint groups from one or more site collections/sites in the farm.
To delete one or more SharePoint groups:

1. Select the object(s) from which you want to delete SharePoint groups.
2. Choose Users and Security > Delete SharePoint Groups.
3. Select the SharePoint group(s) you want to delete as follows:
   a) Select the group(s) from the Available Items list and move them to the Selected Items list.
      Note that all groups defined for the entire site collection display beneath the root site. Groups
      with unique permissions also display beneath the site granting those permissions.
      
      TIP: If your Available Items list is particularly long, you may find it useful to narrow the scope by
      searching based on Group name, site Name, and/or site URL) and searching for the group.

   b) When you have finished adding groups to the Selected Items list, click [Apply].

Now you can either:

- run the operation immediately (by clicking the [Run Now] button)
OR

- complete the Enforce Policy section and **schedule the operation to run at a later time.**

OR

- **save the operation as XML Instructions that can be executed at a later time.**

If you chose the Run Now, option, after the operation has been processed:

- a confirmation message displays at the top of the page, and
- a ControlPoint Task Audit is generated for the operation and displays in the Results section.

If you schedule the operation, a link to the Task Audit is included in the scheduled action notification email.

See also [Auditing ControlPoint Administrator Tasks](#).

### Backing Up and Restoring Site Permissions

The ControlPoint Backup Permissions action lets you back up the permissions of one or more SharePoint sites, which includes:

- permissions granted to users or groups specified in Active Directory or other authentication providers
- permissions granted to SharePoint groups
- membership in SharePoint groups.

The following are *not* backed up:

- Permission level definitions
- SharePoint group definitions
- Active Directory group membership

A separate backup is created for each site within a site collection. For example, if you choose to back up a site collection that contains multiple subsites, a separate backup will be made of the root site and each subsite.

In a multi-farm environment, permissions backups can be created and managed for the home farm only.

#### Restoring Permissions from a Backup

You can restore permissions from a backup using the ControlPoint Manage Permissions Backups feature. You can choose whether or not to restore SharePoint groups that have been deleted, membership in SharePoint groups, and/or Site Collection Administrators.
Changes that are made between the time when permissions are backed up and restored are handled as follows:

- If an object had unique permissions at the time of the backup has since been made inherited, the unique permissions will be restored.
- If a site has been deleted since the backup was made, it will be skipped.
- If it can be determined that a user no longer exists (on the site, Active Directory group, server etc.), permissions for that user will not be restored.
- Any new list or list item has been added since the backup was created will remain intact.
- The permissions of any user who was given direct permissions since the backup was created will be deleted (the user(s) will remain in the SharePoint All People list, however). If you choose to restore group membership, any users added to a SharePoint group since the backup was created will not be deleted. Because SharePoint groups are defined at the site collection level, deleting a user would remove the user's permissions to all sites within the collection that use that group.

### Backing Up Site Permissions

Use the ControlPoint **Backup Permissions** action to back up permissions on one or more SharePoint sites, to maintain the integrity of site security throughout your farm.

For example, you may want to back up permissions:

- for the entire farm on a regular basis (such as weekly)
- to have a “snapshot” of the original permissions set up for a newly created site
- before performing an administrative action that may compromise site security settings.

Permissions are backed up site by site, with permissions for each individual site saved as a separate line item in the data table `xcPermissionsbackup`—in the ControlPoint Administration database (`xcadmin`)—along with the date and time of the operation. Definitions of permissions levels are not backed up.

**NOTE:** Depending on the scope of the operation and the number of objects (sites, lists, and/or list items) with unique permissions, the permissions backup process can be time-consuming and resource-intensive. Therefore, it is recommended that you perform the operation—or schedule the operation to run—when system usage is low.

### To back up site permissions:

1. Select the object(s) containing the sites whose permissions you want to back up.
2. Choose Users and Security > Backup Permissions.

Now you can either:

- run the operation immediately (by clicking the [Run Now] button)

OR
• complete the Enforce Policy section and schedule the operation to run at a later time.

OR

• save the operation as XML Instructions that can be executed at a later time.

If you chose the Run Now, option, after the operation has been processed:

• a confirmation message displays at the top of the page, and

• a ControlPoint Task Audit is generated for the operation and displays in the Results section.

If you schedule the operation, a link to the Task Audit is included in the scheduled action notification email.

See also Auditing ControlPoint Administrator Tasks.

Restoring Site Permissions from a Backup

Use the Manage Permissions Backups action to restore user permissions for one or more sites whose permissions have been backed up. You can choose whether or not to restore from the backup:

• SharePoint groups that may have been deleted

• the membership of SharePoint groups, and/or

• the Site Collection Administrator.

REMINDER: Permissions That are Restored/Not Restored

• Definitions of permissions levels cannot be backed up, and therefore cannot be restored. If a permissions level was deleted from a site since the Backup Date, an error will be reported.

• Any sites that have been deleted since the Backup Date will not be restored, nor will permissions for users who are no longer valid on the server or in Active Directory (that is, deleted or disabled users).

• For any object that currently that has unique permissions but had inherited permissions as of the Backup Date, inheritance will be restored. Conversely, for any object with unique permissions that had inherited permissions as of the Backup date, the unique permissions will be restored.

• The permissions of any user who was given direct permissions since the Backup Date will be deleted. If you choose to restore group membership, however, any user added to a SharePoint group since the Backup Date will not be deleted, as that user may have permissions to other sites in the collection via membership in the group.

• Any lists and list items created after the Backup Date will remain intact.

To restore permissions backups:

1 Select the object(s) whose permissions you want to restore.
2 Choose Users and Security > Manage Permissions Backups.

The Show most recent backups for each site box is checked by default and only the most recent backup for each site within the scope of your selection will display. You can, however, check or uncheck this box as needed.

3 If you want to narrow the list to backups to a specific date range:
   a) Select a Show Backups from and Show Backups until date ( ) and time ( ).
   b) Click [Refresh Display].

4 Check the appropriate restore option(s):
   - **Restore groups** - Check this box if you want any SharePoint groups (and group membership) that have been deleted since the Backup Date to be restored. If you leave this box unchecked, groups will not be restored.
   - **Restore users to groups** - Check this box if you want to restore membership in SharePoint groups that may have changed since the Backup Date. (That is, any deleted users will be restored. Users that have been added to group since the Backup Date will not be deleted, however.) If you leave this box unchecked, only members that have been added to the group since the backup date (if any) will be retained.
     REMINDER: Users who are no longer valid on the server or in Active Directory will not be restored.
   - **Restore Site Administrator** - Check this box if you want to restore the Site Administrator(s) that existed as of the backup date. If you leave this box unchecked, the current Site Administrator(s) will be retained.

5 Highlight the row(s) containing the backups from which you want to restore permissions. To select multiple backups, use the [Shift] and [Ctrl] keys in the conventional manner.

Now you can either:
• run the action immediately, (by clicking the [Restore from selected backup] button)  

OR

• schedule the restore to run at a later time  

OR

• generate an xml file with instructions that can be executed at a later time (by clicking [Save Instructions for Restore]).

If you chose the Run Now, option, after the operation has been processed:

• a confirmation message displays at the top of the page, and

• a ControlPoint Task Audit is generated for the operation and displays in the Results section.

If you schedule the operation, a link to the Task Audit is included in the scheduled action notification email.

See also Auditing ControlPoint Administrator Tasks.

Deleting Permissions Backups

From the Manage Permissions Backups interface you can delete one or more permissions backups.

NOTE: If you want to narrow the list to backups to a specific date range, select a Show Backups from and Show Backups until date ( ) and time ( ), then click [Refresh Display].

To delete selected backup(s):

1. In the Select column, check the box beside each backup you want to delete.*
2. Click [Delete selected backups].
You will be prompted to confirm the deletion before the operation is carried out.

**To delete all backups:**

1. Click `[Select All]`.*
2. Click `[Delete selected backups]`.

You will be prompted to confirm the deletion before the operation is carried out.

*NOTE: If you want to de-select currently selected backups, click `[Reset]`.

### Managing Permissions Inheritance

The ControlPoint Manage Permissions Inheritance action lets you break or restore permissions inheritance of sites, subsites, lists, folders, and items across your SharePoint farm.

**SharePoint Objects Included in the Operation by Default**

The following table identifies the SharePoint objects that are included in the Break/Restore Inheritance operation by default.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Scope</th>
<th>Objects Included by Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore Inheritance</td>
<td>Site Collection</td>
<td>All sites, subsites, lists, folders and items within the selected scope.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: You can use the [Change Selection] option if you want to exclude individual sites, lists, folders, and items.</td>
</tr>
<tr>
<td>Site</td>
<td>Site Collection</td>
<td>The site itself and all lists, folders and items within the site.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: If you have checked the [Include Children] box in the Selection pane (that is, you want to include child sites of the selected site), you can also choose to exclude the selected site itself (so that child sites will inherit from it).</td>
</tr>
<tr>
<td>List</td>
<td>Site Collection</td>
<td>The list itself.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: By default folders and items are not acted upon. You can, however, use the [Change Selection] option to explicitly select any folders, and items you want to include.</td>
</tr>
<tr>
<td>Break Inheritance</td>
<td>Site Collection</td>
<td>All sites and subsites within the selected scope.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: By default, lists, folders, and items are not acted upon. You can, however, use the [Change Selection] option to explicitly select any lists, folders, and items you want to include.</td>
</tr>
</tbody>
</table>
### Operation

<table>
<thead>
<tr>
<th>Operation</th>
<th>Scope</th>
<th>Objects Included by Default</th>
</tr>
</thead>
</table>
| Site      | The site itself and all subsites.  
NOTES:  
· By default, lists, folders, and items are not acted upon. You can, however, use the **Change Selection** option to explicitly select any lists, folders, and items you want to include.  
· If you have checked the **Include Children** box in the Selection pane (that is, you want to include child sites of the selected site), you can also choose to **exclude** the selected site itself (so that child sites will no longer inherit from it). | |
| List      | The list itself.  
NOTE: By default, folders and items are not acted upon. You can, however, use the **Change Selection** option to explicitly select any folders and items you want to include. | |

### To manage permissions inheritance:

1. Select the object(s) for which you want to break or restore inheritance.
2. Choose Users and Security > Manage Permissions Inheritance.
3. Use the information in the following table to determine the appropriate action to take.

<table>
<thead>
<tr>
<th>If you want to ...</th>
<th>Then ...</th>
</tr>
</thead>
</table>
| restore permissions inheritance | select the **Restore Inheritance** radio button.  
| | ![Restore Inheritance](Image)  
| All lists and list items will inherit permissions |
| break permissions inheritance | a. Select the **Break Inheritance** radio button.  
b. Select whether you want to:  
· **Copy Permissions from Parent**  
OR  
· **Leave Permissions Empty**.  
| ![Break Inheritance](Image)  
| Copy Permissions from Parent  
| Leave Permissions Empty |
4 If you initiated the action at the site level and want to act only on child site(s), check the Include Children only (exclude selected sites) box.

Now you can either:

- run the operation immediately (by clicking the [Run Now] button)

OR

- complete the Enforce Policy section and schedule the operation to run at a later time.

OR

- save the operation as XML Instructions that can be executed at a later time.

If you chose the Run Now, option, after the operation has been processed:

- a confirmation message displays at the top of the page, and
- a ControlPoint Task Audit is generated for the operation and displays in the Results section.

If you schedule the operation, a link to the Task Audit is included in the scheduled action notification email.

See also Auditing ControlPoint Administrator Tasks.
Provisioning SharePoint Site Collections and Sites O365

ControlPoint Site Provisioning functionality automates the management of end user requests for new site collections and sites, which are based on "Provisioning Profiles" that you define.

Managing Site Provisioning Profiles

Before an end user can request a new site collection or site, at least one Provisioning Profile must have been created. Once created, the Provisioning Profile becomes available to end users when a request for a new site collection or site is initiated.

To launch the ControlPoint Provisioning Profile Manager:

From the Manager ControlPoint panel, choose Governance Policy Manager and Provisioning > Provisioning Profile Manager.

To create a Provisioning Profile:

1. From the Provisioning Profile Manager main page, choose [Create].
2. Complete the fields on the Build New Provision Profile page as follows:
   - Enter the Profile Name as you want it to display in the Provisioning Profile Manager list.
- Enter the **End User Description** as you want it to display in the Request a Site or Site Collection page.
- Enter the **Profile Description** as you want it to display in the Provisioning Profile Manager list.
- Select a **Base SharePoint Template**.

**NOTE:** The Custom template tab is intended for a future release.

3. If you want to **Attach Additional Profile Settings**, you can
- Click the appropriate link—**Set Site Collection Properties** (if available), Set Site Properties, or Set List Properties—and complete the applicable window.

**NOTE:** If you select **Enforce Policy** and **schedule the operation to run on a recurring basis**, it will be enforced for any site collection or site created using that Profile.

4. Click **[Create]**.

**To edit a Provisioning Profile:**

1. From the Provisioning Profile Manager main page, check the box to the left of the Profile that you want to edit.
2. Click **[Edit]**.
3. Edit the fields on the Edit Provision Profile page as appropriate.
4. Click **[Update]**.

**To delete one or more Provisioning Profiles:**

1. From the Provisioning Profile Manager main page, check the box to the left of the Profile(s) that you want to delete.
2. Click **[Delete]**

You will be prompted to confirm your action before continuing.

**How New Sites and Site Collections Are Requested O365**

An end user can request a new site or site collection as long as:

- the url for the Request Site or Site Collection page has been made available
- the requester can be authenticated in Active Directory as a valid Office 365 user
- the ControlPoint Application Administrator has specified the credentials to use for provisioning request submission.
When the Request Site or Site Collection page is launched, the user will be prompted for login credentials. Once logged in, the user can select from the available Profiles that were created via the ControlPoint Provisioning Profile Manager.

Upon selecting a Profile, the Create Site (or Site Collection) page displays, prompting the requester for the following information:

- a **Title** and **Description** for the new site
- the **Web Site Address** that the requester wants to use for the new site

**NOTE:** The requester must enter a full URL, including the name of the new site. For example, if the requester wants to create a subsite called Blog under mycompany.sharepoint.com/sites/sales, a valid URL might be https://mycompany.sharepoint.com/sites/sales/blog.

The **Requester Name** and **Requester Email address** pre-populate with the login name and email address of the current user. The Requester Email Address can, however, be changed. If the request is for a **Site Collection**, **Primary Site Collection Administrator** and **Primary Site Collection Email Address** fields are pre-populated with the current user’s information, but they can also be changed.
When the requester places the request, ControlPoint validates the information provided by the requester, including that the URL is valid and available. If the validation fails, any error messages display at the top of the form.

If the validation is successful, a confirmation number is generated and displays at the top of the form, and a confirmation email is automatically sent to the requester.

NOTE: Once a request is submitted, it is registered in the Site Creation Requests list on the ControlPoint Configuration Site.

Making Provisioning Profiles Available to End Users O365

After at least one Provisioning Profile has been created, the next step is to make the Request Site or Site Collection page available to end users so they can submit requests for new site collections and sites.

The Request Site or Site Collection Request page is initially accessible via the ControlPoint home page dashboard, in the Resources section.
For non-ControlPoint users, the Request Site or Site Collection page can be accessed via the following URL:

http://<server_name>:<port_number>/_layouts/axceler/CPSiteProvisioning.aspx

(The server machine name is the name of the machine on which the ControlPoint Online application is installed. 2828 is the default port number for ControlPoint Online.)

Before a non-ControlPoint user can submit a site provisioning request, the ControlPoint Application Administrator must specify credentials that have the authority to access ControlPoint and to create site collections and sites in your SharePoint Online environment. See Specifying Credentials to Use for Site Provisioning Requests.

Specifying Credentials to Use for Site Provisioning Requests

Before a non-ControlPoint user can submit a site provisioning request, the ControlPoint Application Administrator must specify credentials that will be used to create site collections and subites in your SharePoint Online environment.

NOTE: To create subsites, the account must be a Site Collection Administrator for every site collection in the tenancy where a site may be provisioned. To create site collections, the account must be an Office 365 Global Administrator.

To specify credentials for Site Provisioning Request submission:

NOTE: Only one one set of credentials can be saved per account type.
1 From the Manage ControlPoint tree, choose Governance Policy Manager and Provisioning > Online Credentials Manager.

2 Click [Create].

From the Add Account drop-down, select the appropriate Account Type:

- Site Collection Administrator (for creating new sites)
- OR
- Global Administrator (for creating new site collections)

Enter the Account Name and Password, then click [Insert].

ControlPoint validates the credentials to ensure that the account name and password are correct and that the account has the appropriate permissions.

**Managing Site Provisioning Requests**

From the Manage Site Provisioning Requests page, you can:

- monitor incoming requests for site collections and sites
- approve or reject the requests, and
- edit request details, such as title, description or url.
To launch the Provisioning Requests Manager:

From the Manage ControlPoint tree, choose Governance Policy Manager and Provisioning > Provisioning Requests Manager.

To edit/view details of a Provisioning Profile:

1. In the Manage Provision Requests grid, check the box to the left of the request that you want to view/edit.
2. Click [Edit].
Note that you can edit the **Title**, **Description**, and **URL** of the request. You can also approve or reject the request by changing the **Request Status**.

If a request is **Rejected**, an email is automatically sent to the requester. If a request is **Approved**, it automatically starts Processing and is **Completed** when the site collection or site is created. Once the site or site collection is created, an email is automatically sent to the requester.

Note that you can edit the **Title**, **Description**, and **URL** of the request. You can also approve or reject the request by changing the **Request Status**.

If a request is **Rejected**, an email is automatically sent to the requester. If a request is **Approved**, it automatically starts Processing and is **Completed** when the site collection or site is created and all of the Additional Profile Settings (properties and Governance Policies) been applied per the new site collection or site. Once the site or site collection is created, an email is automatically sent to the requester.

---

**NOTE:** Additional Profile Settings are applied the next time the scheduled job that has been defined for the operation has run.

2. Click [Update].

**To approve one or more requests without viewing or editing details:**

1. From the Provisioning Request Manager main page, check the box to the left of each request you want to approve.

2. Click [Approve].

**To delete one or more requests:**

1. From the Provisioning Requests Manager main page, check the box to the left of the request(s) that you want to delete.

2. Click [Delete]

You will be prompted to confirm your action before continuing.
Data Analysis and Reporting

ControlPoint offers several advanced tools for analyzing data in the SharePoint environment, including:

- storage used by various SharePoint objects
- site content
- information about users
- trends over a specified time period
- the contents of SharePoint audit and change logs.

An additional tool, the ControlPoint Task Audit, enable you to review ControlPoint actions taken by administrators.

Analysis tools are accessible for various levels of the hierarchy. As with other ControlPoint features, the scope of the analysis is determined by the hierarchical context.

Most analyses can also be configured so that they can be invoked directly from a url, which can be bookmarked, emailed, or placed on a SharePoint site.

NOTE: This chapter describes all of the ControlPoint analysis tools provided by Metalogix. Depending on the configuration of your ControlPoint menus, however, the analysis tools to which you have access, and their location in the menus invoked from the left navigation pane, may vary.

Specifying Parameters for Your Analysis

When you select a ControlPoint analysis tool from the left navigation pane, you are prompted to specify the parameters you want to use. The most common parameters used in various ControlPoint analysis tools are described below.

Cached vs. Real-time Data

Some ControlPoint analyses give you the option of using either cached or real-time data for analyses performed on the farm, one or more Web applications, or site collections.

- Use cached data

If the Use cached data box is checked, your analysis will include data that has been collected by ControlPoint during the last run of Discovery. The advantage of using cached data is that the analysis will be processed more quickly and will not compete for system resources. Because Full Discovery is run on a nightly basis, the use of cached data is often sufficient, especially when the analysis contains data that is not likely to change significantly over the course of a day.

The advantage of using real-time data (when the Use cached data box is unchecked) is that your analysis
will contain the most current information. However, because the data is being captured in real time, the analysis will take longer to process and may tie up system resources.

**IMPORTANT:** For analyses performed on a single site collection or site, real-time data is always used and the **Use cached data** option is disabled. Because data collection within a single site collection or site is less time-consuming, the impact on system resources is minimal.

### Specific Date or Time Period

For analyses that cover a specific time period, you select the time period by specifying a **Start Date** and **End Date**.

Start date: 10/18/2013
End date: 10/18/2013

For analyses that involve **activity**, only cached data is used, since these analyses are based on accumulated summary data collected nightly by SharePoint usage analysis jobs.

For analyses involving other types of data (such as site collection storage) you are given the option of using real-time data.

**IMPORTANT:** Historical data that predates the ControlPoint cache will not be reflected in analysis results. For example, if the ControlPoint cache was created two weeks ago, a maximum of two weeks-worth of data is available for analysis, regardless of the date range you specify. Similarly, any historical data that postdates the last run of Discovery will not be reflected in results. For example, if you request data for a time period that covers the last 30 days and the last time Discovery ran was 10 days ago, analysis results will reflect the time period **up to** the last Discovery run date.

The format that ControlPoint uses to display dates is based on browser settings (rather than server settings). If you want to change the format (from mm/dd/yy to dd/mm/yy for example), go to Internet Options and change the Language Preference.

It is worth noting that deleted sites will display in activity and storage analysis results if they were active during the specified time period.

### Open drill-down Options

For analyses that allow you to drill down to a more detailed ControlPoint analysis, you can choose to display it in a separate window by checking the **Open drill-downs in new window** box.

If you leave this box unchecked, the analysis to which you are drilling down will display in the current
workspace, and parameters from the original analysis will be carried over. You can return to the original analysis by clicking the Back arrow in the report header.

Note that, when you link to a SharePoint page from analysis results, it always displays in a separate window.

**Expanded Results Option**

For most analyses that contain nested data, you have the option of choosing whether or not you want to display results expanded.

If you want to display results at the highest level of detail, leave the **Display with results expanded** box unchecked (the default option). You can then expand items individually, and view, print, or export additional detail for selected items only.

If your analysis contains a lot of nested data and you want to view, search, print, or export all of the analysis detail without drilling down, you may choose to have results display fully expanded by checking the **Display with results expanded** box.

TIP: If you choose to display expanded results and your analysis contains a large amount of data, you can use the Document Map to more easily navigate through results. See [Analysis Results Display](#).

**Additional Parameters for Permissions Analyses**

The following parameters are specific to SharePoint user permissions analyses:

- If you want to limit results to one or more specific users, the **Select users** field allows you to select the users you want to include in your analysis. If you leave this field blank, all users will be included.

  **Select users (blank for all):**

  Mark Twain ; James Joyce ;

  NOTE: You must use real-time (not cached) data if you are selecting users based on a SharePoint User Profile Property.
• If the scope of your analysis includes sites with multiple child objects, you can choose to display all objects (including those whose permissions are inherited) by unchecking the **Show Unique Permissions Only** box.

  ![Show unique permissions only]

  **NOTE:** If this option is checked, only sites with unique (non-inherited) permissions will be included in the results.

• If you want results to include only users who have direct permissions (that is, do not have permissions via a SharePoint group), check the **Include only users with Direct permissions** box.

  ![Include only users with Direct permissions]

  **TIP:** You can use this option to identify "rogue users" who *should* have permissions through membership in a SharePoint group, then initiate an Add User to Groups action directly from analysis results. See [Acting on Search or Data Analysis Results](#).

• If you want results to **Show External Users only**, check this box.

  ![Show external users only]

• If you want to limit results to one or more specific permissions levels, select them from the **Limit to Users with permissions level(s)** list box. (All built-in and custom permissions levels that are currently assigned to at least one user on at least one site within the scope of your analysis display in the this box.)

  **Limit to users with permission level(s):**

  ![Limit to users with permission level(s)]

  If the analyses includes lists and/or items, permissions levels that are assigned to a list/item that are *not* assigned at the site level will not display in the list box. (The list box is populated by data collected by the ControlPoint Discovery process, which does not go below the site level.) A list- or item-level permissions level can, however, be entered in the **Limit by Other Levels** field.

  **Limit by Other levels:**

  ![Limit by Other levels]
• If you want results to include only sites for which anonymous access is allowed, check the **Show Anonymous Access Only** box.

![Show Anonymous Access Only](image)

• If you want a cumulative total of unique users who have permissions for objects within the selected scope, check the **Calculate Total Users with Permissions** box.

![Calculate Total Users with Permissions](image)

**NOTE:** Total Users with Permissions uses data recorded in the ControlPoint Service (xcadmin) database, and is current as of the last Discovery run. If you run the analysis using real-time data, all users are counted in real time, which may significantly increase the amount of time it takes to run the analysis.

### Analysis Results Display

All ControlPoint analysis results displays include a standard header and footer, in addition to analysis-specific detail.

### Analysis Results Toolbar

ControlPoint analysis results pages include a toolbar which contains page navigation, export, and print capabilities.

Above the toolbar are links that enable you to:

- select all objects in analysis results to include in a ControlPoint operation
- download results as a CSV file

![Toolbar with Select All and Download Report Data as CSV options](image)

### Analysis Results Detail

The analysis results detail sections contains summary information, followed by the analysis-specific content.

The summary section includes the parameters used, as well as the name of the user who ran the analysis and the run date and time.
Note that, if the analysis was run using cached data, the date and time that the cache was last refreshed via the Discovery task displays. The information in the analysis is current as of that date and time. If the analysis was run on real-time data, the Cached field will be populated by the value “False.”

You can sort line items in analysis detail for any column that includes an up/down arrow.

**Analysis Results Footer Information**

The analysis footer, which appears on every page of the results, contains the following information:

- the name of the administrator who generated the analysis (which can be useful if results are exported or printed and distributed, since the content of the analysis reflects that administrator’s permissions)
- the number of pages in the analysis (you can scroll through multi-page results from the navigation toolbar in the search results header), and
- the date and time when the results were generated.
Selection Summary

The Selection table is repeated at the end of the Results section. This information is included in printed or exported results, as a helpful reminder of the item(s) included in your analysis.

<table>
<thead>
<tr>
<th>Include</th>
<th>Type</th>
<th>Name</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Alpha Snack Foods (4)</td>
<td><a href="http://2010foundation/sites/alpha">http://2010foundation/sites/alpha</a></td>
<td>2010SharePoint &gt; SharePoint &gt; Sites &gt; Alpha Snack Foods</td>
</tr>
<tr>
<td>✓</td>
<td>Delta Transportation</td>
<td><a href="http://2010foundation/sites/delta">http://2010foundation/sites/delta</a></td>
<td>2010SharePoint &gt; SharePoint &gt; Sites &gt; Delta Transportation</td>
</tr>
</tbody>
</table>

Working with Data Analysis Results

From data analysis results you can perform any of the operations described in the following table.

<table>
<thead>
<tr>
<th>If you want to ...</th>
<th>Then ...</th>
</tr>
</thead>
</table>
| print analysis results | from the results toolbar:  
  a) Click the print preview icon ( ).  
  b) Click the print icon ( ).  
  (Printed results will contain only the data that is currently expanded.) |
| export analysis results | choose an Export to the selected format option from the drop-down, then click the Export link.  
  NOTE: If you export to Excel, all data will be exported, regardless of whether it is expanded. If you export to an Acrobat (PDF) file, only data that is currently expanded will be exported. |
| download raw analysis result data to a CSV file that can be imported into another program for further examination | click the Download as CSV hyperlink in the results toolbar.  
  Download Report Data as CSV  
  This option differs from the csv option in the Export... drop-down in that it provides all of the raw data (including object GUIDs and internal field names, for example) used to create the report. This may be useful for |
<table>
<thead>
<tr>
<th>If you want to ...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>troubleshooting or for more in-depth analysis.</td>
<td></td>
</tr>
<tr>
<td>perform a ControlPoint action or analysis within the current workspace</td>
<td>use the procedure for <a href="#">Acting on Search or Data Analysis Results</a>.</td>
</tr>
<tr>
<td>return to the results of an analysis from which you drilled-down</td>
<td>click the Back button in the results toolbar.</td>
</tr>
</tbody>
</table>

**Linking to SharePoint Pages and Other ControlPoint Analyses from Analysis Results**

When run interactively*, from the results of most ControlPoint analyses, you can:

- open relevant SharePoint pages
- generate applicable ControlPoint analyses for the same scope and parameters.

Links to SharePoint pages always open in a separate browser window or tab.
Links to ControlPoint analyses may either open in a separate browser window/tab or in the current workspace, depending on the value of the *Open drill-downs in new window*.  

* Generally, these links are not functional in analysis results that have been exported, although in some cases they may be.

### Acting on Search or Data Analysis Results

From ControlPoint search or data analysis results, you can open a SharePoint page or initiate a ControlPoint action or another analysis for selected objects.

This feature can facilitate the performance of a variety of administrative tasks. For example, you can generate a Site Permissions analysis to identify the users who have been granted permissions directly, then initiate the appropriate action (such as Add User to SharePoint Group).

**To select objects on which to perform a ControlPoint action or analysis:**

1. Click the **Select** link for the object on which you want to act.

```
User Rights

Select  User  Display

  - Clients
  - ControlPoint Configuration Site
  - Alpha Snack Foods

Select
```

**NOTE:** To select all objects in the results list, click the **Select All** link in the Results header.
The Selection Builder opens in a separate window.

NOTE: If you want the Selection Builder to remain open in a static location in the browser window, click the Pin On icon ( ) in the upper left corner of the Selection Builder window. To disable this feature, click Pin Off ( ).

2 If you want to select additional objects, either:
   - click the Select All link in the analysis results Select column for each additional item you want to add to the Selection Builder.
   OR
   - from within the Selection Builder, use the procedure for Changing Your Selection.

3 Choose the applicable SharePoint page or ControlPoint operation from the Selection Builder menu.
   - Note that the rules for selecting objects from the left navigation pane apply here as well. For example, only options that are appropriate for the selected object(s) are available.

NOTE: The Selection Builder will appear minimized until you click Restore ( ). If you close the
Selection Builder, your current selection(s) will be cleared.

**Generating a SharePoint Summary Report**

The SharePoint Summary report provides a comprehensive summary of the components (servers, services, Web applications, site collections, and sites) in the SharePoint Online environment currently being managed in ControlPoint, along with various size statistics.

You also have the option of including details about servers in your SharePoint farm—such as storage, performance, and usage statistics—which is collected from Windows Performance Monitor. This option can, however, significantly increase the time it takes to generate the report.

---

**NOTE:** For a server’s details be included in report results, the Axceler Service account must have permissions to request status information from the server. Details can be found in the *ControlPoint Administration Guide*.

---

**To generate a SharePoint Summary report:**

From the SharePoint Hierarchy panel select the top node, then from the context menu or ribbon Home tab choose SharePoint Summary:

- SharePoint Summary > Select parameter(s) to act on

View activity for: Last 30 days

- Display with results expanded

Note that the **View activity for**: dropdown is disabled as it does not apply for this report.

Now you can either:

- run the operation immediately (by clicking the **Run Now** button)

OR

- **schedule the operation to run at a later time**.

OR

- **save the operation as XML Instructions that can be executed at a later time**.

The SharePoint Summary consists of the following sections:

- a summary of farm components
- Servers and Services
- Web Applications
- Service Application Association (SharePoint 2010 farms only)

**Farm Components Summary**

The top of the report displays the total number of servers, Web applications, site collections, and sites in the farm.

Note that the Total # of Sites includes root sites (whereas in the SharePoint Hierarchy, the number that displays in parentheses beside a site collection excludes the root site).

**Servers and Services**

If you chose to Show Servers Details, the Servers and Services section lists all of the servers in the farm, as well as all of the services currently installed on each server. Storage, performance, and usage details also display.

**Note:** Information reported varies, depending on the nature of the server. For example, Web Requests are not relevant for a SQL server. Depending on how WMI captures the information, if a statistic is irrelevant for the server, the value will display as either N/A or 0.

**Web Applications**

In addition to the Web application name and url, the Web Applications section displays the following statistics for each individual Web application, as well as aggregated totals for the entire farm:

- the number of:
  - Site Collections
  - Sites - which includes root sites and any subsites that have been created
  - Lists - which includes both user-created (visible) lists and internal (hidden) lists, such as galleries, that are necessary for the functioning of the site, and
  - Files - which includes web pages as well as documents
- Size, (in MB) - the total size of the Web application's content, which:
  - does not include elements such as metadata, logs, free space, and other overhead
  - is not the disk size of the content database
- If all site collections within a Web application have quotas:
  - Free Space
  - % Usage

**Note:** If there are site collections within a Web application that do not have quotas set, "N/A" will display in the Free Space and % Usage columns.

- Number of Requests for the specified date or date range.
EXCEPTION: If you have WSS only installed, only cumulative data is available. For more detail, see Variations in Activity Data.

When expanded, the following information about each Web application's content database(s) displays:

- the corresponding IIS application pool and the source account that runs the application pool
- the name of both the content database and the server on which it resides
- the current number of site collections in the database, and
- the maximum number of site collections allowed in the database.

Service Application Associations (SharePoint 2010)

If you are running SharePoint 2010, two additional sections are included in report results:

The Service Application Associations per Web Application section lists each Web application, along with the application Proxy Group to which it is mapped. When expanded, each Service Application associated with the Web application is listed along with its Status.

The Web Applications Associated With Service Applications section lists each of the Service Applications that have been associated with one or more Web applications. When expanded, all of the Web applications with which the Service Application is associated are listed.

Object Summary

The top of the report displays the total number of site collections and sites in the environment.

| Total # of Site Collections: | 51 |
| Total # of Sites: | 245 |

Site Collection Detail

The Site Collection Details section displays the following statistics for each individual site collection, as well as aggregated totals for the entire environment:

- the number of Sites, Lists, and Files in the collection
- the Size of the collection as well as Free Space and % Usage of allocated storage space.

Analyzing Site Collection Storage

The Site Collection Storage Analysis provides storage statistics for selected site collections, including:

- the distribution of storage among Web applications selected for analysis, and
the number of top site collections (that is, site collections with the scope of your analysis using the most storage).

**To generate a Site Collection Storage Analysis:**

1. Select the object(s) on which you want to perform the analysis.
2. Choose Storage > Site Collection Storage Analysis.
3. Specify the parameters for your analysis.
   
   Note that, in addition to the "standard" parameters, a **Limit display to** must be specified. The value in this field (which is 10 by default, but may be changed), represents the number of sites using the most storage space that you want to examine more closely. These sites are listed in a separate section at the bottom of the analysis results.

   ![Limit display to:](image)

Now you can either:

- run the operation immediately (by clicking the [Run Now] button)
- schedule the operation to run at a later time.
- save the operation as XML Instructions that can be executed at a later time.

The Site Collection Storage analysis consists of the following sections:

- Web Applications
- Size Distributions
- Storage Usage
- Top Site Collections

**Web Applications Section**

The Web Applications section lists the Web application(s) within the scope of your analysis, along with the following statistics for individual Web applications and cumulative totals:

- the number of site Collections, Sites, Lists, and Files.
- the Size, in megabytes (MB) of storage used.

**NOTE**: Size includes content but excludes logs, metadata and other storage overhead. It is not meant to reflect the size of the content database.

When expanded, these statistics display for individual site collections, along with:

- the Content DB used by the site collection
- Quota in megabytes (MB)
- %Usage relative to the quota.

<table>
<thead>
<tr>
<th>Web applications</th>
<th>Collections</th>
<th>Content DB</th>
<th>Sites</th>
<th>Lists</th>
<th>Files</th>
<th>Size (MB)</th>
<th>Quota (MB)</th>
<th>% Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ControlPoint Configuration Site</td>
<td>1</td>
<td>WSS_CONTENT_ACCELER</td>
<td>1</td>
<td>15</td>
<td>400</td>
<td>4.53</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>SharePoint - 80</td>
<td>14</td>
<td>48</td>
<td>478</td>
<td>6,158</td>
<td>327.91</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alpha Site</td>
<td>8</td>
<td>89</td>
<td>1,529</td>
<td>284.23</td>
<td>0</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Beta Site</td>
<td>27</td>
<td>157</td>
<td>1,623</td>
<td>19.42</td>
<td>100</td>
<td>19.42</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delta Site</td>
<td>1</td>
<td>19</td>
<td>260</td>
<td>5.95</td>
<td>100</td>
<td>5.95</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIA Site</td>
<td>2</td>
<td>25</td>
<td>310</td>
<td>1.87</td>
<td>100</td>
<td>1.87</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Site</td>
<td>1</td>
<td>21</td>
<td>348</td>
<td>1.81</td>
<td>100</td>
<td>1.81</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Model Site</td>
<td>1</td>
<td>15</td>
<td>134</td>
<td>1.71</td>
<td>100</td>
<td>1.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gamma Site</td>
<td>1</td>
<td>19</td>
<td>291</td>
<td>1.7</td>
<td>100</td>
<td>1.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Iota Site</td>
<td>1</td>
<td>19</td>
<td>238</td>
<td>1.61</td>
<td>100</td>
<td>1.61</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eta Site</td>
<td>1</td>
<td>19</td>
<td>237</td>
<td>1.61</td>
<td>100</td>
<td>1.61</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Size Distributions and Storage Usage Sections**

The Size Distributions section consists of a pie chart that depicts the size distribution among the Web applications within the scope of your analysis. (If you generated the report for a single Web application, the chart will appear solid.)

The Storage Usage section consists of a bar chart that shows the amount of storage space used by
each Web application relative to the Web application’s quota.

NOTE: If a quota has not been set for the Web application, Used Space will not be captured.

### Top Site Collections by Size

This section shows statistics for the site collections using the most storage space. The number of site collections that display in this section is determined by the value you specified for [Limit display to](#).

<table>
<thead>
<tr>
<th>Select</th>
<th>Site Collection</th>
<th>Web Application / Content DB</th>
<th>Owner</th>
<th>Files</th>
<th>Size (MB)</th>
<th>Quota (MB)</th>
<th>% Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select</td>
<td>Alpha Snack Foods</td>
<td>SharePoint - 80</td>
<td>AXCELER</td>
<td>TEST:development</td>
<td>1,529</td>
<td>294.23</td>
<td>0</td>
</tr>
<tr>
<td>Select</td>
<td>Beta Aquatics</td>
<td>SharePoint - 80</td>
<td>BELLUM:Administrator</td>
<td>1,623</td>
<td>19.42</td>
<td>100</td>
<td>19.42</td>
</tr>
<tr>
<td>Select</td>
<td>Delta Transportation</td>
<td>SharePoint - 80</td>
<td>BELLUM:Administrator</td>
<td>200</td>
<td>5.95</td>
<td>100</td>
<td>5.95</td>
</tr>
<tr>
<td>Select</td>
<td>ControlPoint Configuration Site</td>
<td>SharePoint - 80</td>
<td>BELLUM:Administrator</td>
<td>382</td>
<td>3.33</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>Select</td>
<td>CIA</td>
<td>SharePoint - 80</td>
<td>BELLUM:Administrator</td>
<td>310</td>
<td>1.87</td>
<td>100</td>
<td>1.87</td>
</tr>
</tbody>
</table>

**Totals**

<table>
<thead>
<tr>
<th></th>
<th>Files</th>
<th>Size (MB)</th>
<th>Quota (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4,104</td>
<td>314.8</td>
<td>300</td>
</tr>
</tbody>
</table>

### Analyzing Storage by File Type

The Storage by File Type analysis provides both a graphical and tabular representation of the amount of storage used by various file types in the content database(s), both by file size and count. You have the option of including all file types, or including/excluding those with specified file extensions.

You can also drill down to a Most/Least Storage Analysis for a selected file type, to view files using the largest amount of storage.

**NOTE:** This analysis encompasses files within SharePoint content databases. Files stored within the file system, such as SharePoint Features, are not included.
To generate a Storage by File Type analysis:

1. **Select the object(s) you want to include in your analysis.**

2. Choose Storage > Storage by File Type.

3. Specify the following parameters for your analysis:
   - If you want include or exclude specific file types:
     - Specify whether you want to **Include Extensions** or **Exclude Extensions**.
     - Enter the file extension(s) you want to include or exclude in the **File Extensions** field.
     - Enter multiple extensions as a comma-separated list.

   **NOTE:** If you want include all file types, leave the File Extensions field blank. If you chose Exclude Extensions, you must enter at least one file extension.

Now you can either:

- run the operation immediately (by clicking the [Run Now] button)

OR

- **schedule the operation to run at a later time.**

OR

- **save the operation as XML Instructions that can be executed at a later time.**

Analysis results include:

- two pie charts that depict the **Storage by File Size** and **Storage by Type** for the selected scope and file types.

- a listing that includes the **Extension(s)**, **Total Files** and **Total Size (MB)** for each file type.
Click an Extension(s) hyperlink to generate a Most/Least Storage analysis that shows the files with that extension that use the most storage (the number of which was specified in the Number of Files to Show in Drill-down).

<table>
<thead>
<tr>
<th>Extension(s)</th>
<th>Total Files</th>
<th>Total Size (Mb)</th>
</tr>
</thead>
<tbody>
<tr>
<td>.pdf</td>
<td>254</td>
<td>171.133</td>
</tr>
<tr>
<td>.docx</td>
<td>21</td>
<td>46.182</td>
</tr>
<tr>
<td>.docx</td>
<td>47</td>
<td>10.111</td>
</tr>
</tbody>
</table>

**Analyzing Trends**

For a single farm, Web application, or site collection, you can analyze trends over a specified time period in:

- site count, and/or
- storage.

**To generate a Trends analysis:**

1. Select the object for which you want to analyze trends.

   NOTE: You can only analyze trends for one object (farm, Web application, or site collection) at a time. If you multi-select, only the object on which you right-clicked will apply.

2. Use the information in the following table to determine the appropriate action to take.

<table>
<thead>
<tr>
<th>If you want to analyze trends in ...</th>
<th>Choose ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>site count</td>
<td>Content &gt; Trend Analysis for Site Count</td>
</tr>
<tr>
<td>storage</td>
<td>Storage &gt; Trend Analysis for Storage.</td>
</tr>
</tbody>
</table>

3. Specify the following parameters for your analysis:

   a) Enter or select a **Start Date** and **End Date** for your analysis.

      The date range you select determines the time intervals captured in the analysis, as described in the following table.

<table>
<thead>
<tr>
<th>If the time period you specified is ...</th>
<th>Then the Trend Analysis will be reported ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>up to 60 days</td>
<td>by Day</td>
</tr>
<tr>
<td>between 61 and 364 days</td>
<td>by Week</td>
</tr>
<tr>
<td>365 days or greater</td>
<td>by Month.</td>
</tr>
</tbody>
</table>
b) If you want to change the **Statistics to Graph**, select a different value from the drop-down.

c) If you want your graph to include a line that smooths out short-term fluctuations, check the **Include moving Average** box.

The default value for **Moving average period** (days) is 7, which represents the number of days within a given week. This value is useful for many business users who can expect less activity, for example, on the weekend. You can, however, change this value to measure moving average for a different time period. For example, if you generally experience week-to-week fluctuations over the course of a month, you may choose to set the Moving average period to 31.

Now you can either:

- run the operation immediately (by clicking the [Run Now] button)

OR

- **schedule the operation to run at a later time.**

OR

- **save the operation as XML Instructions that can be executed at a later time.**

Trend Analysis results consist of two graphs:

- The Trend Analysis bar graph includes the statistics for the selected criterion. (Note that if you selected ALL from the **Statistics to graph** drop-down, a separate graph will be included for each).

Below are examples of Trend Analyses by Day reports (including a 7-day moving average) for Storage, and Site Count over the same 28-day time period.

**Storage Trend Analysis**

![Storage Trend Analysis Graph](image-url)
The second graph is a line graph that shows statistics for both options (storage and site count) in terms of a percentage over the course of the selected time period. Note that the maximum value (100%) represents the most storage used and largest site count over the selected time period.

### Analyzing Managed Metadata Usage

The Metadata Usage analysis lets you analyze the use of managed metadata as list/library columns in your SharePoint environment. You can group results by site or by term set and you have the option to include usage count and the individual items in lists or libraries that use the metadata.

**To generate a Managed Metadata Usage analysis:**

1. Select the object(s) whose managed metadata usage you want to analyze.
2. Choose Content > Managed Metadata Usage.
3 Specify the parameters for your analysis. Use the information in the following table for guidance.

If you ... | Then ...
---|---
want results to include only metadata with term sets OR terms that contain a specific text string | • enter the string in **Show only Metadata of TermSets/Terms containing** field.

NOTE: You can enter multiple text strings as a comma-separated list.

• choose the applicable **Select by** option (to indicate whether you want ControlPoint to search for TermSet or Term)

want results to include the number of list items that have a value in the column that uses the metadata | check the **Show item usage count** box.

want results to include the actual list items that have a value in the column that uses the metadata | check the **Show items in list or library** box.

NOTE: If you check this box, ControlPoint must iterate through all list items. Depending on the scope of your analysis and the number of items within that scope, processing time may increase noticeably.

want to group results by term set rather than by site | uncheck the **Group by Site** box.

Now you can either:

- run the operation immediately (by clicking the **Run Now** button)

OR

- **schedule the operation to run at a later time.**

OR

- **save the operation as XML Instructions that can be executed at a later time.**

If you chose to group results by site:

- The top level of the analysis shows each of the Web applications and sites within the scope of your analysis that use managed metadata

- When expanded, the following information displays each list that uses managed metadata, along
with the following information:

- the name of the Column referencing the Metadata
- the Term Store, Term Group, and Term Set
- the Term specified for the list column (if applicable)

**NOTE:** The Term column will also show item-level terms only if the Show items in list or library box.

- if the Item Usage count parameter was checked, the number of items for which the column has been populated with metadata.

If you chose to group results by TermSet:

- The top level of the analysis shows each Term Store providing the metadata, followed by each Term Group and Term Set.
- When expanded, the following information displays for each term set:
  - the site that uses the metadata
  - for each list that uses the metadata:
    - the name of the Column Referencing the Metadata
    - if the Item Usage count parameter was checked, the number of items for which the column has been populated with metadata.
• the **Term** specified for the column (if applicable)

NOTE: The Term column will also show item-level terms only if the **Show items in list or library** box.

Note that if you have customized a term set for the site collection, SharePoint assigns the name of the Term Group.

To open the SharePoint site that uses the metadata, click on the site url.

To open SharePoint list settings page for a list, click on the list name.

**Analyzing Users and Permissions**

ControlPoint provides the following tools that allow you to examine permissions of SharePoint users throughout your farm:

- **Site Permissions** shows the permissions of users for selected sites
- **Site List Permissions** shows user permissions for individual lists and list items within a site.

An additional analysis, **Comprehensive Permissions**, show permissions for all sites, lists, and optionally list items within a single result set.

NOTE: In addition to showing user permissions at the individual site level, all Site Permissions analyses include any Web application policy permissions users may have.

**Finding Orphaned Domain Users**

If you are using Active Directory as the authentication method for your SharePoint Online environment, the Orphaned Domain Users analysis lists users who currently have permissions in SharePoint but are no longer valid in the Active Directory.
Users Evaluated as Potential Orphans

ControlPoint evaluates users as potential orphans if they are disabled in and/or deleted from Active Directory but are found in:

- a SharePoint permission entry at any level (site, subsite, list, library, folder, or item)
- a site collection’s All People list, and/or
- a Site Collection Administrator’s list (via the All People List).

ControlPoint does not evaluate names in Web application policies, the Farm Administrator list, or any custom SharePoint list that may contain user names.

Users That Are Not Reported as Orphans

ControlPoint does not report a user as being orphaned if it is considered valid by SharePoint (that is, if a user who is not in the All People list can still be validated by the SharePoint People Picker). Active Directory entries that are considered valid by SharePoint (and therefore are not reported as orphaned by ControlPoint) include:

- expired accounts, and
- locked accounts (i.e., accounts for which the allowable threshold for failed login attempts has been exceeded).

To generate an Orphaned Domain Users analysis:

1. Select the object(s) you want to include in your analysis.
2. Choose Users and Security > Orphaned Domain Users.
3. Specify the parameters for your analysis.
   - Note that you have the option of limiting your results only to users who are either disabled in or have been deleted from Active Directory. If you accept the default option, Show all orphans, both types of users will be included.
4. If you want ControlPoint to automatically delete all users returned by the analysis on the home farm, check the Automatically delete users after analysis has run (in home farm only). Note that, in a multifarm environment, this action cannot be carried out on a remote farm.
CAUTION: If you check this box, ControlPoint will automatically submit one or more Delete User jobs to the ControlPoint scheduler. The number of jobs submitted depends on the number of users to be deleted, and the number of users processed in a job is determined by the ControlPoint Setting OrphanDeleteBatchSize. The first job will be scheduled to run 30 minutes after the analysis has finished processing. Because this action cannot be undone, you may want to back up user permissions before executing the operation. (You also have the option of deleting jobs before they have run via the Schedule Monitor.)

Now you can either:

- run the operation immediately (by clicking the [Run Now] button)

OR

- schedule the operation to run at a later time.

OR

- save the operation as XML Instructions that can be executed at a later time.

When expanded, a list of rights for each orphaned user displays the same information as the User Rights section of the Site Permissions analysis.

**Disabled Accounts as Orphans**

Users whose accounts have been disabled (or disabled and renamed) in the Active Directory are normally considered orphans by both SharePoint and ControlPoint and are annotated as such in analysis results. This annotation is intended to help you in evaluating whether or not such users really should be considered orphans in accordance with your organization's policies.

If an account has been both disabled and renamed, the annotation will include the original name, followed by the string DISABLED, RENAMED; and the new name. (ControlPoint will not consider a renamed account orphaned if it is also active, expired, or locked.)

NOTE: Although it is not a common practice, it is possible for restricted reads and other permissions to be placed on entries in the Active Directory. This can affect ControlPoint's ability to detect disabled accounts. Specifically, if an account has been disabled AND cannot be read by the Axceler Service Account, then both SharePoint and ControlPoint will treat that account as valid (not an orphan).

**To delete orphaned user permissions from analysis results:**

Use the information in the following table to determine the appropriate action to take.

CAUTION: If you have any doubt as whether a user is truly orphaned, it is recommended that before you delete permissions, you verify his/her existence and status in the Active Directory.
<table>
<thead>
<tr>
<th>If you want to delete permissions for ...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>a specific orphaned user</td>
<td>click a <strong>User</strong> hyperlink to initiate a ControlPoint Delete User Permissions action.</td>
</tr>
</tbody>
</table>

The Delete User Permissions page opens in a separate browser window, with the **Delete Users** field pre-filled with the selected user(s). Note that you need to run the action without validating the user, as the account now longer exists in Active Directory.

| all orphaned users as an interactive tasks | click the **Delete All** hyperlink at the top of the analysis results section. |

### Analyzing Site Permissions

The Site Permissions analysis lets you examine the permissions that one or more users have for selected sites, including external users.

**To generate a Site Permissions analysis:**

1. Select the object(s) you want to include in your analysis.
2. Choose Users and Security > Site Permissions.
3. Specify the parameters for your analysis.
   - Note that, in addition to the "standard" parameters, you have the option to **Group by** Sites (the default) or Users.

   ![Group by options]

Now you can either:

- run the operation immediately (by clicking the **[Run Now]** button)

OR
• schedule the operation to run at a later time.

OR

• save the operation as XML Instructions that can be executed at a later time.

The top level of the User Rights section lists the Web application(s) within the scope of your analysis.

When expanded, a list of users with permissions for the site collection or site displays, along with the following information:

• the login name of the SharePoint User

• the user's permission level(s), as indicated by a plus sign (+) in the applicable column(s), which may include:
  ▪ the site collection's Admin group
  ▪ the five default SharePoint permission levels:
    ▪ Full Control
    ▪ Design
    ▪ Contribute
    ▪ Read
    ▪ Limited.

NOTE: If a user has a template-specific or custom permission level, it is recorded in the Other column.

By default, the report lists:
- users with direct permissions, and
- users with membership through SharePoint groups.

The **Display Name/Group** column shows the display name of each user whose permissions are direct or through membership in a SharePoint group. If a display name does not exist for the user, the user’s login name will display in brackets < >.

Note that in the following example, the external user is identified by his external email address.

### Analyzing Site Lists Permissions

The Site Lists Permissions analysis lets you examine the permissions of users for individual lists within a selected site, including external users.

**NOTE**: List permissions are also included as part of the Comprehensive Permissions analysis. You can also view permissions for items within a selected list by running a [Permissions by List Item analysis](#).

**To generate a Site Lists Permissions analysis:**

1. Select the site whose list permissions you want to analyze.
   
   **NOTE**: You can only analyze list permissions for one site at a time. If you multi-select, only the site on which you right-clicked will apply.

2. Choose Users and Security > Site Lists Permissions. Use the information in the following table to determine the appropriate action to take.

3. Specify the parameters for your analysis.

Now you can either:

- run the operation immediately (by clicking the [Run Now] button)

OR

- **schedule the operation to run at a later time.**

OR

- **save the operation as XML Instructions that can be executed at a later time.**

The top level of the Site Lists Permissions analysis shows all of the lists used on the site, along with the
following information:

- the **Security** type (Inherited or Unique)
- the number of **Items** in the list
- the number of **Items with Unique Permissions**.

**NOTE:** If you chose to **Show unique permissions only**, results will include any list that contains *items* with unique permissions (even if the list itself has inherited permissions).

When expanded, the following information displays for each list:

- each **User** with permissions to the List item(s)
- if applicable, the **SharePoint Group** via which the user has permissions (users who have direct access are appropriately identified)
- the number of **Accessible Items** for that user, and
- the user’s permission level(s). A plus sign (+) displays in the applicable column(s), which may include any of the five default SharePoint permission levels:
  - **Full Control**
  - **Design**
  - **Contribute**
  - **Read**
  - **Limited**.
NOTE: If a user has a template-specific or custom permission level, it is recorded in the Other column.

Analyzing Permissions by List Item

The Permissions by List Item analysis lets you examine user permissions for folders and items within selected lists.

NOTE: List item permissions are also included as part of Comprehensive Permissions analysis.

To generate a Permissions by List Item analysis:

1. Select the list(s) whose item permissions you want to analyze.
2. Choose Users and Security > Permissions by List Item.
3. If you want to analyze only specific items within the selected scope, select the items you want to analyze.
4. Specify the parameters for your analysis.

Now you can either:
• run the operation immediately (by clicking the [Run Now] button)

OR

• schedule the operation to run at a later time.

OR

• save the operation as XML instructions that can be executed at a later time.

The first row of the result set includes the following information about the list itself:

• an icon that identifies the list type (document library, calendar, task list, etc.).
• the name of the list
• the List Security type (Inherited or Unique)
• the number of Items in the list
• the number of Items with Unique Permissions.

When the first row is expanded, each user with permissions for the list is displayed, along with the following information:

• the name of the SharePoint User
• the number of Accessible Items (that is, the number of items within the list for which the user has permissions)
• the user’s permission level(s) for the list itself, as indicated by a plus sign (+) in the applicable column(s), which may include:
  ▪ the site collection’s Admin group
  ▪ the five default SharePoint permission levels:
    ▪ Full Control
    ▪ Design
    ▪ Contribute
    ▪ Read
    ▪ Limited.
NOTE: If a user has a template-specific or custom permission level, it is recorded in the Other column.

The remaining rows contain detailed permissions information for each folder and item within the list.

Click a list, folder, or item name to open the SharePoint Permissions page.

Note that in the following example, the external user is identified by his external email address.

Analyzing Comprehensive Permissions

The Comprehensive Permissions analysis shows the permissions that users including external users have to selected sites as well as lists (and optionally, list items) within those sites.

If you want to analyze site-level permissions only (with the option of drilling down to list permissions for each user individually), you can run a Site Permissions analysis instead.

NOTE: The Comprehensive Permissions analysis always uses real-time (not cached) data.

To generate a Comprehensive Permissions analysis:

1. Select the object(s) on which you want to perform the analysis.
2. Choose Users and Security > Comprehensive Permissions

3. Specify the parameters for your analysis.
   Note that, in addition to the "standard" parameters, you have the option to Group by Sites (the default) or Users.

   ![Group by: Sites Users]

   **NOTE:** By default, permissions for list items are excluded from the analysis. You can, however, choose to Include List Items. Be aware however, that processing time may increase significantly.

Now you can either:

- run the operation immediately (by clicking the [Run Now] button)

   OR

- schedule the operation to run at a later time.

   OR

- save the operation as XML Instructions that can be executed at a later time.

Because Comprehensive Permissions analyses are always run on real-time data, if your analysis encompasses multiple users, sites, lists, and/or list items, the analysis may run very slowly and the result set may be very large. Therefore, you may want to consider running it by schedule.

In addition to the same site-level permissions (Site Security) shown in the Site Permissions by Site analysis, the User Rights section also shows the same list-level and optionally, item-level permissions (List Security) shown in the Site Lists Permissions analysis.

### Analyzing SharePoint Groups

The SharePoint Groups Analysis provides details about membership and permissions of SharePoint groups within one or more site collections and/or sites.

**To generate a SharePoint Groups analysis:**

1. Select the object(s) for which you want to analyze SharePoint groups.

2. Choose Users and Security > SharePoint Group Analysis.

3. Specify the parameters for your analysis.
   In addition to the "standard" parameters for permissions analyses, you can limit results to:

   - SharePoint groups whose name include a specific text string
   - groups with no members and/or with no permissions or only groups with both members and permissions
You can also choose whether to **Include lists and list items** in results.

**CAUTION:** If you chose to include lists and list items, the analysis may take significantly longer to run and may generate a much larger set of results.

**SHAREPOINT GROUP ANALYSIS**

Now you can either:

- run the operation immediately (by clicking the **[Run Now]** button)

OR

- **schedule the operation to run at a later time.**

OR

- **save the operation as XML Instructions that can be executed at a later time.**

The SharePoint Group Analysis consists of the following sections:

- Membership
- Permissions

**Membership Section**

The Membership section lists each site collection within the scope of your analysis.

When expanded the following information displays:

- each **SharePoint Group** within the site collection
- the **No of users** in the group.
- a plus sign (+) identifying each group that **Has Permissions.**
When expanded, each Member login name and Display Name is listed.

### Permissions Section

The Permissions section lists each site within the scope of your analysis.

When expanded, a Site Security summary row indicates whether site security is Inherited or Unique. Each SharePoint Group within the site is listed, along with a plus sign (+) identifying each of its permissions. Any custom permissions levels are recorded in the Other column.

Note that in the following example, the external user is identified by his external email address.
Auditing Activities and Changes in Your SharePoint Environment

SharePoint captures activities and changes to the environment via the following mechanisms:

- the Audit Log, which focuses on activities performed by SharePoint users.
- the Change Log, which focuses on changes made to the SharePoint environment.

ControlPoint provides functionality that enables you to view contents of audit logs and change logs, which is not currently available in native SharePoint.

Events Captured in SharePoint Logs

The following tables identify the log(s) where different types of events are recorded and the event codes used to identify them.

NOTE: Be aware that some events may not appear immediately in analysis results, as it can take several minutes for them to be recorded in the SharePoint log.

### Add/Delete Site Collections, Sites, Libraries and Lists

<table>
<thead>
<tr>
<th>Event</th>
<th>Where Recorded (ControlPoint Event Type)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Site collection added</td>
<td>Change Log <em>(Add)</em></td>
</tr>
<tr>
<td>• Site added</td>
<td></td>
</tr>
<tr>
<td>• Library or list added</td>
<td>NOTE: It may take several minutes for an added site to appear in the Change Log.</td>
</tr>
<tr>
<td>• Site deleted</td>
<td>Audit Log <em>(Delete/Delete Child)</em></td>
</tr>
<tr>
<td>• Library or list deleted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NOTE: A Delete event is reported from the perspective of the object itself. A Delete Child event is reported within the scope of the object's parent.</td>
</tr>
<tr>
<td></td>
<td>• Change Log <em>(Delete)</em></td>
</tr>
</tbody>
</table>

### Add/Delete Document and List Items

<table>
<thead>
<tr>
<th>Event</th>
<th>Where Recorded (ControlPoint Event Type)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document or list item added</td>
<td>• Audit Log <em>(Update)</em></td>
</tr>
<tr>
<td></td>
<td>• Change Log <em>(Add)</em></td>
</tr>
<tr>
<td>Document or list item deleted</td>
<td>• Audit Log <em>(Delete/Delete Child)</em></td>
</tr>
<tr>
<td></td>
<td>NOTE: A Delete event is reported from the perspective of the object itself. A Delete Child event is reported within the scope of the object's parent.</td>
</tr>
<tr>
<td></td>
<td>• Change Log <em>(Delete)</em></td>
</tr>
<tr>
<td>Document or list item restored</td>
<td>• Audit Log <em>(Undelete)</em></td>
</tr>
<tr>
<td>Event</td>
<td>Where Recorded (ControlPoint Event Type)</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Change Log (Restore)</td>
</tr>
</tbody>
</table>

**Other Actions on Document and List Items**

<table>
<thead>
<tr>
<th>Event</th>
<th>Where Recorded (ControlPoint Event Type)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document opened/downloaded</td>
<td>Audit Log (View)</td>
</tr>
<tr>
<td>List item viewed</td>
<td></td>
</tr>
<tr>
<td>List item properties viewed</td>
<td></td>
</tr>
<tr>
<td>Document or list item edited</td>
<td>Audit Log (Update)</td>
</tr>
<tr>
<td>Document or list item properties edited</td>
<td>Change Log (Update)</td>
</tr>
<tr>
<td>Item checked in/checked out</td>
<td>Audit Log (Check In/Check Out)</td>
</tr>
<tr>
<td>Items moved to another location in the site</td>
<td>Change Log (Move)</td>
</tr>
<tr>
<td>Items copied to another location in the site (using</td>
<td></td>
</tr>
<tr>
<td>the Send To menu entry)</td>
<td>Audit Log (Update)</td>
</tr>
<tr>
<td>Item accessed as part of a workflow</td>
<td>Audit Log (Workflow)</td>
</tr>
</tbody>
</table>

**Add/Delete/Change Users and Permissions**

<table>
<thead>
<tr>
<th>Event</th>
<th>Where Recorded (ControlPoint Event Type) (SharePoint Event Code)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site security inheritance broken</td>
<td>Audit Log (Turn Off Inheritance from Parent) (SecRoleBindBreakInherit)</td>
</tr>
<tr>
<td></td>
<td>Change Log (Add Assignment) (AssignmentAdd)</td>
</tr>
<tr>
<td>Site security inheritance restored</td>
<td>Audit Log (Turn On Inheritance from Parent) (SecRoleBindInherit)</td>
</tr>
<tr>
<td></td>
<td>Change Log (Delete Assignment) (Assignment)</td>
</tr>
<tr>
<td>Permission level inheritance restored</td>
<td>Change Log (Delete Assignment) (Assignment)</td>
</tr>
<tr>
<td>Site permission level created</td>
<td>Audit Log (Create Permissions) (SecRoleDefCreate)</td>
</tr>
<tr>
<td></td>
<td>Change Log (Add Role) (RoleUpdate)</td>
</tr>
<tr>
<td>Site permission level deleted</td>
<td>Audit Log (Remove Permissions) (SecRoleDefDelete)</td>
</tr>
<tr>
<td></td>
<td>Change Log (Delete Role) (RoleUpdate)</td>
</tr>
<tr>
<td>Site Permission level changed</td>
<td>Audit Log (Modify Permissions) (SecGroupCreate)</td>
</tr>
<tr>
<td>Event</td>
<td>Where Recorded (ControlPoint Event Type) (SharePoint Event Code)</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| User or SharePoint group permission changed | - Audit Log (Change Permissions) (SecRoleBindUpdate)  
|      | - Change Log (Add Assignment and/or Delete Assignment)  
|      | (AssignmentAdd and/or Assignment)  |
| SharePoint group created | - Audit Log (Create Group) (SecGroupCreate)  
| | - Change Log (Add) |
| SharePoint group deleted | - Audit Log (Delete Group) (SecGroupDelete)  
| | - Change Log (Delete) |
| Member added to SharePoint group | - Audit Log (Add Member to Group) (SecGroupMemberAdd)  
| | - Change Log (Add Member) (MemberAdd) |
| Member deleted from SharePoint group | - Audit Log (Delete Member from Group) (SecGroupMemberDelete)  
| | - Change Log (Delete Member) (MemberDelete) |

**Add Content Types and Columns**

<table>
<thead>
<tr>
<th>Action</th>
<th>Where Recorded (ControlPoint Event Type) (SharePoint Event Code)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Type added</td>
<td>Audit Log (Change Profile) (ProfileChange)</td>
</tr>
<tr>
<td>Column added</td>
<td>Audit Log (Change Schema) (SchemaChange)</td>
</tr>
</tbody>
</table>

**SharePoint Search Activity**

<table>
<thead>
<tr>
<th>Event</th>
<th>Where Recorded (ControlPoint Event Type)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SharePoint search performed</td>
<td>Audit Log (Search)</td>
</tr>
</tbody>
</table>

**Audit Settings**

<table>
<thead>
<tr>
<th>Event</th>
<th>Where Recorded (ControlPoint Event Type) (SharePoint Event Code)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit settings changed</td>
<td>Audit Log (Change Mask) (AuditMaskChange)</td>
</tr>
</tbody>
</table>

**Analyzing Audit Log Contents**

The ControlPoint Audit Log analysis extends SharePoint's built-in audit logging by letting you easily view entries written to the audit log. You can focus your analysis on specific event types, and even limit the scope to include only certain objects (sites, lists, documents, etc.).
Audit logging must be enabled for each site collection whose events you want to log.

**How ControlPoint Online Gathers Audit Log Data**

When an Audit Log analysis is run, ControlPoint Online prompts SharePoint to gather the requested data. The data collected by SharePoint is saved to a document library at the root site of each site collection within the scope of the analysis. The library to which this data is saved is defined by the ControlPoint Configuration Setting `HostedAuditLogReportList`.

![Diagram of SharePoint hierarchy]

**To generate an Audit Log analysis:**

1. **Select the object(s) for which you want to view audited events.**
   
   NOTES:
   
   - If the scope of your analysis includes site collections that have been deleted, audit events associated with that site collection will no longer exist.
   - As with all ControlPoint analyses, if you initiated the analysis from the farm or site collection level, all child items will be included by default. If you initiated the analysis at the site level, only information for that site (not its subsites) will be included. You can, however, use the Change Selection option to further refine your scope.

2. Choose Audit and Alerts > Audit Log.

3. Specify one or more of the following parameters for your analysis:
   
   - select both a **Start** and **End date** and time for which you want to report. The time period for which you can generate an audit log analysis depends on how many days audit data is retained. The ControlPoint default is 0 (meaning that audit data is never deleted), but the ControlPoint Application Administrator can specify a different value via ControlPoint Configuration Settings.
   - select the **User(s)** whose actions you want to audit (or leave blank for all users)
   - enter a **relative URL** (note that you can enter a url down to the item level; you can also use an asterisk (*) at the beginning and end of a url as wildcards)

**EXAMPLES**
- sites/al*
- sites/alpha/shared documents/xcrSummaryReport.pdf

- select one or more Event types from the list box. Refer to the topic Events Captured in SharePoint Logs for guidance in selecting the appropriate event type(s).

  CAUTION: Although you have the option of viewing ALL events, if you select this option your result set may be extremely large. One reason is that SharePoint records some events (such as a View) as a series of several events. Also, some event types (such as Update) may encompass a wide variety of events.

- If you want the report generated by SharePoint to be deleted from the SharePoint library(ies), check Delete report generated by SharePoint.

  NOTE: ControlPoint saves the SharePoint report to a file that includes a date stamp. Therefore, if you leave this box unchecked, a new report will be saved to the library(ies) each time the analysis is run (that is, it will not replace a previously-saved report).

Now you can either:

- run the operation immediately (by clicking the [Run Now] button)

OR

- schedule the operation to run at a later time.

OR

- save the operation as XML Instructions that can be executed at a later time.

**Information in the Audit Log analysis**

The Audit Log analysis contains the following information:
- the **Date** and time that the event occurred
- the **User** responsible for the event
- the **Event** type
- the **Scope** of the event, which may be:
  - site collection (Site)
  - site (Web)
  - List
  - Folder, Document, or List Item
- the name of the **Site Collection** and **Site** on/within which the event occurred.
- the relative **URL** for the list or document/item.

Depending on the event type, additional detail may display beneath each line item.

### Analyzing Change Log Contents

The ControlPoint Change Log lets you view the contents of SharePoint change logs for one or more selected event types.

**To generate a Change Log analysis:**

1. Select the object(s) for which you want to view change log entries.
2. Choose Audit & Alerts > Change Log Analysis.
3. Specify one or more of the following parameters for your analysis:
   - select both a **Start** and **End date** ( ) and time ( ) for which you want to report
The time period for which you can generate a change log analysis depends on how many days change log data is retained. ControlPoint relies on the history maintained by SharePoint. SharePoint for Office 365 retains Change Log data for 60 days.

- **enter a relative URL** (note that you can enter a url down to the item level; you can also use an asterisk (*) at the beginning and end of a url as wildcards)
  
  EXAMPLES
  
  - sites/al*
  - sites/alpha/shared documents/SharePointPlanning.docx

- select one or more **Event** types from the list box. Refer to the topic [Events Captured in SharePoint Logs](#) for guidance in selecting the appropriate event type(s).

Now you can either:

- run the operation immediately (by clicking the **[Run Now]** button)

  OR

- **schedule the operation to run at a later time.**

  OR

- **save the operation as XML Instructions that can be executed at a later time.**
Information in the Change Log Analysis

The ControlPoint Change Log Analysis contains the following information:

- the Date and time that the event occurred
- the Scope of the event
- the Event type
- the individual the event was Performed By

NOTE: For many event types, SharePoint change logging does not record the user who performed the event. In such cases, the value "None" will appear in the Performed By column.

- the name of the Site Collection and Site on/within which the event occurred.
- the URL for the item (if applicable).

The ControlPoint Task Audit

The ControlPoint Task Audit is an analysis tool that summarizes one or more of the ControlPoint actions that have been performed by administrators over a specified time period.

By default, the Task Audit report is accessible from the Manage ControlPoint panel. An action-specific Task Audit Report is also displayed automatically after a ControlPoint action is carried out.

NOTE: In a multi-farm installation, the Task Audit includes actions performed on both home and remote farms.
To generate a Task Audit:

1. From the Manage ControlPoint panel, choose Schedule Management and Logging > ControlPoint Task Audit.
2. Specify the following parameters for your analysis:
   - Either
     - Enter the **StartDate** and **EndDate**, or
     - click the Calendar icon and select the date(s).
   - (Optional) If you want to search for a specific text string, complete the **Search for** field. You can enter a full or partial:
     - site name or url
     - action name, or
     - action description
   - For example, by entering the words "Site Theme" in the **Search for** field, your results will be limited to tasks that involved modifying a site theme.

   ![Search for: Permissions](image)

   Select an **Administrator** from the drop-down. (If you want report results to include all administrators in the list, select <ALL>).

   Note that the drop-down list includes only administrators who have performed a ControlPoint action within that farm.

   - Select a **Task Type** from the drop-down.
NOTE: The Task Type list is populated with the types of actions that have actually been performed by administrators. For example, if a Delete User Permissions action has never been performed, it will not appear in the list. If you want to include all available options in the report results, select <ALL>.

If you chose the Run Now, option, after the operation has been processed:

- a confirmation message displays at the top of the page, and
- a ControlPoint Task Audit is generated for the operation and displays in the Results section.

If you schedule the operation, a link to the Task Audit is included in the scheduled action notification email.

See also Auditing ControlPoint Administrator Tasks.

**Information in the Task Audit Report**

The Task Audit Report contains the following information for each task:

- the Task Type
- the username of the administrator that the task was Performed by
- the Date and time when the task was performed, and
- a summary of the parameters chosen for the action.

When expanded, a more detailed description of a task displays, which lists:

- site collections or sites on which the action was carried out, and
• any special notes or errors (such as "Security is inherited - no processing is done").

Table:

<table>
<thead>
<tr>
<th>Task Type</th>
<th>Performed By</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete User Permissions</td>
<td>acelextest\testbenchacelexel</td>
<td>3/3/2014 3:23 PM</td>
</tr>
</tbody>
</table>

Note that:

• As with other ControlPoint analyses, only actions taken on sites you have permissions to manage within ControlPoint display in audit report results.

• Sites for which the administrator who performed the action does not have permissions to manage are not acted upon, and therefore are not captured in the audit report.

Viewing Logged Errors

The Logged Errors Report lets you view the contents of the ControlPoint Services (xcAdmin) database error log for a specified date range. You can use this detail with guidance from Metalogix Support to diagnose potential issues in your environment.

To view logged errors:

1. From the Manage ControlPoint panel, choose Schedule Management and Logging > Logged Errors Report
2. Select a Start date and End date representing the time period for which you want to view logged errors.

Now you can either:

• run the operation immediately (by clicking the [Run Now] button)
OR

- schedule the operation to run at a later time.

OR

- save the operation as XML instructions that can be executed at a later time.

Logged Error Report results contain a time-stamped entry for each error logged within the specified date range, followed by detailed error text.

Analyzing List Properties

The List Properties analysis provides information about one or more lists in your farm, including:

- the properties of the list, including versioning and advanced settings
- audit settings that are/are not enabled for the list.

To generate a List Properties analysis:

1. Select the object(s) you want to include in your analysis.
2. Choose Configuration > List Properties.
3. If you want results to include only lists that meet one or more specific criteria, specify one or more of the parameters described in the following table.
| If you want results to include only lists... | Then ...
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>whose name contains a specific text string</td>
<td>enter the text string in the <strong>List Name contains</strong> field.</td>
</tr>
<tr>
<td></td>
<td>List Name Contains: client</td>
</tr>
<tr>
<td>that have a particular version setting</td>
<td>select from the <strong>Versions Setting</strong> drop-down.</td>
</tr>
<tr>
<td></td>
<td>Version Settings:</td>
</tr>
<tr>
<td></td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>No Versioning</td>
</tr>
<tr>
<td></td>
<td>Major Versions Only</td>
</tr>
<tr>
<td></td>
<td>Major and Minor Versions</td>
</tr>
<tr>
<td></td>
<td>Any Versioning</td>
</tr>
<tr>
<td></td>
<td>List Type:</td>
</tr>
<tr>
<td></td>
<td>Contacts List</td>
</tr>
<tr>
<td></td>
<td>Data Connection Library</td>
</tr>
<tr>
<td></td>
<td>Discussion Board</td>
</tr>
<tr>
<td></td>
<td>Document Library</td>
</tr>
<tr>
<td></td>
<td>Events List</td>
</tr>
<tr>
<td>of one or more specific types</td>
<td>select from the <strong>List Types</strong> drop-down.</td>
</tr>
</tbody>
</table>

Now you can either:

- run the operation immediately (by clicking the **[Run Now]** button)

OR

- **schedule the operation to run at a later time.**

OR

- **save the operation as XML Instructions that can be executed at a later time.**
The top level of the analysis lists each Web application, site collection, site, and list within the scope of your analysis, along with the list's **Base Type**.

When expanded, the following information is displayed for each list:

- **list Properties**, including versioning and advanced settings detail

  ![List Properties](image)

  - **Versioning**
    - Require Content Approval: False
    - Minor Version Limit: 3
    - Version History Type: MajorVersion
    - Draft Visibility Type: Reader
    - Major Version Limit: 3
    - Require Checkout: False

  - **Advanced Settings**
    - Enable Attachments: False
    - Allow Management of Content Types: True
    - Read Permissions: ModifyAll
    - Display on Quick Launch: True
    - Write Permissions: ModifyYourOwn
    - Enable Audience Targeting: False
    - View Modes: Threaded, Flat, Subject, RichView

- **all of the available Audit Settings**, with settings that are currently enabled for the list identified by a plus sign (+).
NOTE: Audit settings that are inherited from the site collection are flagged with >.

<table>
<thead>
<tr>
<th>Audit Settings</th>
<th>Lists, Libraries and Sites - Events to audit</th>
<th>Documents and Items - Events to audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled?</td>
<td>Editing content types and columns</td>
<td>Opening or downloading documents, viewing items in lists, or viewing item properties</td>
</tr>
<tr>
<td></td>
<td>Searching site content</td>
<td>Editing items</td>
</tr>
<tr>
<td></td>
<td>Editing users and permissions</td>
<td>Checking out or checking in items</td>
</tr>
<tr>
<td></td>
<td>Deleting child objects</td>
<td>Moving or copying items to another location in the site</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deleting or restoring items</td>
</tr>
</tbody>
</table>

- list Columns settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Column Type</th>
<th>Column Description</th>
<th>Content Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval Status</td>
<td>Moderation Status</td>
<td>Moderation Status</td>
<td>N/A</td>
</tr>
<tr>
<td>Approver Comments</td>
<td>Multiple lines of text</td>
<td>Multiple lines of text</td>
<td>N/A</td>
</tr>
<tr>
<td>Attachments</td>
<td>Attachments</td>
<td>Attachments</td>
<td>N/A</td>
</tr>
<tr>
<td>Body</td>
<td>Multiple lines of text</td>
<td>Multiple lines of text</td>
<td>Discussion, Message</td>
</tr>
<tr>
<td>Body Was Expanded</td>
<td>Computed</td>
<td>Computed</td>
<td>Discussion, Message</td>
</tr>
<tr>
<td>Content Type</td>
<td>Single line of text</td>
<td>Single line of text</td>
<td>Discussion, Message</td>
</tr>
<tr>
<td>Content Type Id</td>
<td>Content Type Id</td>
<td>Content Type Id</td>
<td>N/A</td>
</tr>
<tr>
<td>Copy Source</td>
<td>Single line of text</td>
<td>Single line of text</td>
<td>N/A</td>
</tr>
<tr>
<td>Correct Body To Show</td>
<td>Computed</td>
<td>Computed</td>
<td>Discussion, Message</td>
</tr>
<tr>
<td>Created</td>
<td>Date and Time</td>
<td>Date and Time</td>
<td>N/A</td>
</tr>
<tr>
<td>Created By</td>
<td>Person or Group</td>
<td>Person or Group</td>
<td>N/A</td>
</tr>
<tr>
<td>Discussion Subject</td>
<td>Computed</td>
<td>Computed</td>
<td>Discussion, Message</td>
</tr>
<tr>
<td>Discussion Title</td>
<td>Lookup</td>
<td>Lookup (information already on this site)</td>
<td>Discussion, Message</td>
</tr>
</tbody>
</table>

Generating a OneDrive Summary Report

If you The OneDrive Summary report lets you view OneDrive for Business usage information for personal sites to which you have administrator privileges, including "Share With Me" documents.

To generate this report, the ControlPoint Application Administrator must explicitly choose to include OneDrive site collections in the SharePoint Hierarchy. (However, doing so may significantly increase SharePoint Hierarchy load time, especially if there are a large number of OneDrive site collections in the environment.) Contact Metalogix Support for details.

To generate a OneDrive Summary Report:

1. Select the OneDrive site collection(s) (or the OneDrive Site Collections node if you want to include all OneDrive site collections that you administer).
2 Choose OneDrive > OneDrive Summary.

3 If you want to Include item level permissions, check this box.

NOTE: If you choose this option, processing time may increase, especially if the scope of your selection contains a large number of site collections and/or documents.

Now you can either:

- run the operation immediately (by clicking the [Run Now] button)

OR

- schedule the operation to run at a later time.

OR

- save the operation as XML Instructions that can be executed at a later time.

Analysis results include the following information about each OneDrive site collection in the scope of your selection:

- the following General Info About Shared Documents:
  - the owner of the site collection
  - the document name, owner, and URL of each "Share With Me" document on the selected site(s).
  - If you chose to Include item level permissions, the following additional information displays
    - # Shared Documents
    - # Private Documents
    - # Total Documents
    - % of Shared Documents
  - the name, owner, and URL for "Share With Me" Documents.
Scheduling a ControlPoint Operation

The ControlPoint scheduler lets you set up ControlPoint operations to run in the background at a specified date and time, such as when system resource usage is low. Depending on your ControlPoint permissions, you can schedule:

- an Advanced Search
- any ControlPoint analysis
- most ControlPoint actions
- a full or partial Discovery.

This feature is especially useful for:

- operations that might take a significant amount of time to complete (such as an analysis run on a large farm)
- operations that you want to run during off-peak hours (such as moving an active site)
- enforcing corporate or regulatory policies (for example, by ensuring that user permissions are always set at the proper levels)
- analyses that you want to run and distribute on a regular basis (such as weekly site activity or storage usage).

Results of scheduled ControlPoint analyses can be sent to email distribution lists and/or posted to a SharePoint document library as a .pdf, an Excel formatted spreadsheet, or a csv file. Individual data sets within analyses can also be saved as SharePoint lists for use in creating dashboards.

ControlPoint uses a different (typically larger) limit on the number of line items that can be returned when an analysis is run on a scheduled basis than when run interactively. ControlPoint Application Administrators can, however, modify this limit.

NOTE: In a multi-farm installation, operations can only be scheduled for the home farm.

Scheduling a Recurring Analysis for Which a Specific Date Range or Time Period was Selected

If a ControlPoint analysis is scheduled to run on a recurring basis and includes a date range or time period, the ControlPoint scheduler will interpret it as a relative date range or time period (that is, relative to the date when the scheduled job is run). The first time the scheduled job runs, the analysis will cover the date range specified in the Parameters section. For subsequent job runs, the date range will be updated accordingly.

EXAMPLES:
If you initiate an Audit Log analysis on a Monday for a date range that covers the previous week, then schedule it to run on a recurring basis:

- the first time the scheduled job runs, the analysis will include data for the first week in January (that is, the week you specified)

- the second time the scheduled job runs (at the end of the following week), the analysis will include data for the second week in January

- and so on.

- If you schedule a SharePoint Summary Report to run every 30 days, the analysis will include activity that occurred 30 days ending on the date the scheduled job runs, regardless of the date on which
the report was initiated.

How Scheduled Jobs are Handled

The ControlPoint scheduler is driven by the Windows scheduled task that has been configured using the ControlPoint Utility (xcUtilities.exe.) This task both checks for and initiates the execution of scheduled jobs. The task performs these activities every time it runs. (For information on configuring and running the ControlPoint Scheduler, see the ControlPoint Online Administration Guide.)

Creating a Scheduled Job

To schedule a ControlPoint operation:

1. After initiating and specifying the parameters for a ControlPoint operation, open the Schedule section.

   Audit log Analysis

   General Job Information
   - Job Name
   - Description
   - Output File Name
   - Output Type
   - Include Date Time stamp in file name

   Schedule Details
   - Date: 10/10/2012 11:09 AM
   - Recurring
   - Run Every
   - Hours
   - Until: 10/10/2012 12

   Distribution Details
   - Send To
   - Subject
   - Message
   - Destination Farm
   - Add to Library List
   - Send to Admins
   - Send to Site Collection Admins
   - Create Reports by Selection Hierarchy

   Schedule
2 Enter a Job Name and Description.

TIP: Choose a brief but descriptive name that uniquely identifies the job. This will make it easier for you to identify it in the Schedule Monitor and Scheduled Jobs Report. If you choose to have the output posted to a SharePoint document library, the Job Name will also be used as the document Title.

3 If you want the job to be active, make sure the Active box is checked.

NOTE: Once a scheduled job has been added, it can be activated or deactivated as needed.

4 If you want to change the Output File Name, overwrite the default name.

CAUTION: The same default Output File Name is used for every action or analysis of a particular type. For example, whenever you schedule a Site Permissions by Site analysis, the default output file name is xcrRightsBySite, regardless of its scope, or who requested it. It is possible to have more than one job with the same output file name. Keep in mind, however, if more than one job with exactly the same output file name is posted to the same document library, an existing document will be overwritten with a more recent document with the same name.

5 For ControlPoint analyses only:

a) If you want the date and time that the job is run to be appended to the file name, click the Include Date Time stamp in the file name box. (This will enable you to retain a historical record of analysis results that may be used as a record of compliance with policies or regulations.)

b) If different than the default, select an Output Type from the drop-down.

NOTE: If you choose CSV, output will be in the form of raw analysis data that can be imported into another program for further examination.

6 Complete the Schedule Details as follows:

<table>
<thead>
<tr>
<th>If you want to ...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>run an operation one time only</td>
<td>Enter or select a Start date ( ) and time ( ).</td>
</tr>
</tbody>
</table>
If you want to ... | Then ...
---|---
run an operation at regular intervals | 
  a. For **Start**, enter the *first* date (📅) and time (⏲️) that you want the job to run.
  b. Click the **Recurring** box.
  c. For **Run every**:
  - enter the interval (as a positive integer) at which you want the job to run
  - select an interval type (Hour, Day, or Month)
  d. For **Until**, enter or select the *last* date (📅) and time (⏲️) that you want the job to run.

NOTE: Dates and times correspond to those of the server on which the ControlPoint scheduler is running.

7 Complete the **Distribution Details**. Use the information in the following table for guidance.

<table>
<thead>
<tr>
<th>If you want to ...</th>
<th>Then ...</th>
</tr>
</thead>
</table>
| have a notification email sent to one or more recipients when the job completes* (and, in the case of an analysis, have output included in the email as an attachment) | complete the **Send to**, **Subject**, and **Message** fields. (The **From** field will automatically be populated with the email address specified when the ControlPoint Online application was originally installed.)

NOTE: You can either use the SharePoint People Picker as you would when selecting users on which to perform a ControlPoint action or analysis, or enter one or more email addresses (separated by semicolons), in the **Send to** field.

| have analysis results posted to a SharePoint document library | Complete the **Add to Library or List** field as follows:
  - Click [Select] to display the Destination Selection Page pop-up dialog, and select a document library from the Destination Farm Tree. (Note that only lists and libraries within the current farm for which you have Full Control access display).
  - Select a library from the tree (You can also enter a full or partial **Name** or **URL** to narrow your selection). |
If you want to ...

<table>
<thead>
<tr>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image.png" alt="Diagram" /></td>
</tr>
</tbody>
</table>

- Click [OK] to dismiss the dialog and populate the field with the full url path to the selected library.

NOTE: When a document is placed into a SharePoint document library, the Output Filename becomes the document Name, and the Job Name becomes the document Title.

8 To save the job, click [Schedule].

Once a scheduled job has been created, it can be accessed via the Schedule Monitor.

## Monitoring Scheduled Jobs

The Schedule Monitor lets you view the status of scheduled jobs over a specified date range. From the Schedule Monitor you can link to pages that let you:

- view/edit the details of a scheduled job
- delete scheduled jobs
- link to detailed run history of a job
- update Full Discovery and/or Scheduler windows jobs

### To access the Schedule Monitor:

1 From the Manage ControlPoint panel, choose Scheduled Management and Logging > Schedule Monitor.
By default, the Schedule Monitor grid displays jobs that are scheduled to run within the next seven days.

Schedule Monitor > Select parameter(s) to act on

2. If you want to change the default date range, do one of the following:
   - To include jobs within a specified date range:
     a) Enter or select a From "Next Run Date" and To "Next Run Date"
     b) Click [Refresh Display].
   - To include all jobs regardless of the run date, click [Set range to show all dates].
     NOTE: Next Run Date identifies:
     - the next date/time a Pending job is scheduled to run
     - the last date/time a Retired or Inactive job ran
     - the start date/time that an in-process job started running.

3. Select one or more Status values from the list box. Use the information in the table below for guidance.

   NOTE: You can select multiple status values using the [CTRL] or [SHIFT] in the conventional manner. If you want to view all scheduled jobs for the specified date range, select All.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>All jobs that are scheduled to run within the specified date range. Pending jobs include:</td>
</tr>
<tr>
<td></td>
<td>- one-time jobs that have not yet run AND</td>
</tr>
<tr>
<td></td>
<td>- recurring jobs that have not yet reached their End Date.</td>
</tr>
<tr>
<td>Running</td>
<td>All scheduled jobs that are currently running (as long as the specified date range includes the current date).</td>
</tr>
</tbody>
</table>
### Status Description

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cancelling</td>
<td>All running jobs for which the current instance is in the process of being cancelled.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>All jobs for which the last running instance was cancelled.</td>
</tr>
<tr>
<td>Inactive</td>
<td>Jobs that are not currently active but were created or last ran during the specified date range.</td>
</tr>
<tr>
<td>Retired</td>
<td>Jobs that finished running within the specified date range. Retired jobs include:</td>
</tr>
<tr>
<td></td>
<td>- one-time jobs that have already run AND</td>
</tr>
<tr>
<td></td>
<td>- recurring jobs that have reached their End Date.</td>
</tr>
</tbody>
</table>

4. If you want to further filter your results, use the information in the following table for guidance.

<table>
<thead>
<tr>
<th>If you want to ...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>exclude site admin-specific &quot;sub-jobs&quot; that are created when a scheduled job is created with the Create Reports by Selection Hierarchy box checked</td>
<td>check the Exclude Child Jobs box.</td>
</tr>
<tr>
<td>include only jobs of one or more specific types (Actions, Alerts, and/or Reports) (all job types are included by default)</td>
<td>highlight the job type(s) you want to include in the list box.</td>
</tr>
<tr>
<td>display only jobs whose name includes a specified text string</td>
<td>complete the Job Name Includes: field with a full or partial job name.</td>
</tr>
</tbody>
</table>

![Schedule Monitor Filter Settings](image)

![Auto Refresh Settings](image)
The Schedule Monitor displays the following information:

- Job Name
- Job Type
- an indication of whether the job is Active (checked) or inactive (unchecked)
- Schedule Status (Pending, Running, Retired, or Inactive)
- Scheduled Start date and time
- the Schedule End date and time which, for recurring jobs, displays the last date and time that the job is scheduled to run.

NOTE: For one-time jobs, the Schedule End date and time (which displays as an hour later than the Schedule Start) has no significance.

- a checkbox indicating whether the job is one-time (unchecked) or Recurring (checked)
- for recurring jobs, the Interval and Interval Type (Hour, Day, Week or Month)
- Last Run Date and time
- Last Run Status (Complete, Failed, Started, Cancelling, or Cancelled)
- Next Run Date, which identifies:
  - the next date/time a Pending job is scheduled to run
  - the last date/time a Retired or Inactive job ran
  - the start date/time that an in-process job started running.
- the User who scheduled the job.
- an indication of whether or not the scheduled job was created with the Run by hierarchy option
- if the job is an instance of a ControlPoint Governance Policy, the name of the Policy Instance.

You can:

- sort by clicking on a column header
- change the order of columns by dragging and dropping.

From the Schedule Monitor you can:

- set the Schedule Monitor grid to Auto Refresh
- open a job for viewing/editing
- view a job's run history
- cancel or delete one or more jobs
- update Full Discovery and/or Scheduler windows jobs.

Viewing/Editing a Scheduled Job

From the Schedule Monitor, you can access a scheduled job whose details you want to view or edit.
To access a scheduled job's details:

From the Schedule Monitor, click the job’s Edit link.

The job opens in a separate browser window.

To edit the job:

1. Modify the appropriate fields within the Schedule or Enforce Policy section.
2. To save changes, click [Update].

Viewing a Scheduled Job's History

From the Schedule Monitor, you can view the run history of a scheduled job. In the case of scheduled actions (including alerts), you can generate a ControlPoint Task Audit to view more detail about the job.

To view the history of a scheduled job:

- From the Schedule Monitor or Scheduled Jobs Report, click the job’s Last Run link.

- From a scheduled job’s detail page, click the [View History] button.

The Schedule History includes the following information:

- Run Start date and time
- Run End date and time
- process Status (Started, Completed, or Failed)
- in the case of a Failed job, a Message citing the reason for the failure.

As shown in the example below, a separate entry exists for each run of a recurring job. You can sort by either Run Start or Run End date by clicking the up/down arrows in the column header.
To view a ControlPoint Task Audit for a completed action:

Click the link (Completed or Failed) in the Status column.

See also Auditing ControlPoint Administrator Tasks.

NOTE: This link is valid for actions only (not Discovery or analysis jobs)

Canceling or Deleting a Scheduled Job

From the Schedule Monitor you can:

- cancel a running instance of a scheduled job

OR

- completely delete one or more scheduled jobs.

NOTE: If you delete a job that has already run, any history associated with the job will also be deleted.

REMINDE: Delete and Cancel options are disabled if Auto Refresh is enabled.

To stop a running instance of a scheduled job:

NOTE: You can only stop instances of jobs that are currently running, and this action does not delete either the job itself or any future instances of a recurring job.
1. In the Select column, check the box beside each running job instance you want to stop.*
2. Click [Stop Selected].

**To delete one or more scheduled jobs:**
1. In the Select column, check the box beside each job you want to delete.*
2. Click [Delete Selected].

You will be prompted to confirm the deletion before the operation is carried out.

**To delete all scheduled jobs:**
1. Click [Select All].
2. Click [Delete Selected].

You will be prompted to confirm the deletion before the operation is carried out.

*NOTE: If you want to de-select currently selected jobs, click [Reset].

### Updating Full Discovery and Scheduler Windows Jobs

As part of the initial configuration of ControlPoint Online, the following tasks are created in the Windows Task Scheduler on the server where ControlPoint Online is installed:

- the **ControlPoint FullDiscovery job**, scheduled by default to run once a day to populate the ControlPoint data cache.
- the **ControlPoint Scheduler Job**, scheduled to run by default ever 10 minutes to check for and initiate the execution of operations scheduled via the ControlPoint Scheduler.

You can activate/deactivate and change the default start time and/or frequency with which these jobs run via the Schedule Monitor Windows Jobs view.

**CAUTION:** Full Discovery and Scheduler are application-wide jobs. Changing the start time and/or frequency will impact all of ControlPoint.

**To update Full Discovery and/or Scheduler Windows Jobs:**

1. From the Schedule Monitor, select the **Windows Jobs** radio button.
2. Click the Edit icon for the job whose schedule you want to update.
3. Update the Start date, time, and/or run frequency, as applicable.

4. Click [Update].

**Generating a Scheduled Jobs Report**

The Scheduled Jobs Report provides the same information as the Schedule Monitor.

**To generate a Scheduled Jobs Report:**

1. From the Manage ControlPoint panel, choose Schedule Management and Logging > Scheduled Jobs Report.
NOTE: Next Run Date identifies:

- the next date/time a Pending job is scheduled to run
- the last date/time a Retired or Inactive job ran
- the start date/time that an in-process job started running.

2 Select one or more Status values from the list box. Use the information in the table below for guidance.

NOTE: You can select multiple status values using the [CTRL] or [SHIFT] in the conventional manner. If you want to view all scheduled jobs for the specified date range, select All.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
</table>
| Pending | All jobs that are scheduled to run within the specified date range. Pending jobs include:  
- one-time jobs that have not yet run  
AND  
- recurring jobs that have not yet reached their End Date. |
| Running | All scheduled jobs that are currently running (as long as the specified date range includes the current date). |
| Cancelling | All running jobs for which the current instance is in the process of being cancelled. |
| Cancelled | All jobs for which the last running instance was cancelled. |
| Inactive | Jobs that are not currently active but were created or last ran during the specified date range. |
| Retired | Jobs that finished running within the specified date range. Retired jobs include:  
- one-time jobs that have already run  
AND  
- recurring jobs that have reached their End Date. |

3 If you want to further filter your results, use the information in the table below for guidance.
If you want to ... | Then ...  
--- | ---  
exclude site admin-specific "sub-jobs" that are created when a scheduled job is created with the Create Reports by Selection Hierarchy box checked | check the Exclude Child Jobs box.  
include only jobs of one or more specific types (Actions, Alerts, and/or Reports) (all job types are included by default) | highlight the job type(s) you want to include in the Include Job Type(s) list box.  
display only jobs whose name includes a specified text string | complete the Job Name Includes: field with a full or partial job name.  

Now you can either:  
- run the operation immediately (by clicking the [Run Now] button)  
OR  
- schedule the operation to run at a later time.  
OR  
- save the operation as XML instructions that can be executed at a later time.  

From Scheduled Jobs Report results you can view a job's run history.
Saving, Modifying and Executing Instructions for a ControlPoint Operation

All schedulable ControlPoint operations can be saved in an XML file as "instructions" and executed at a later time. If an operation has parameters that are modifiable, you can modify them in the XML file before execution.

NOTE: Currently you cannot run instructions for multi-farm operations.

Saving Instructions

To save Instructions for a ControlPoint operation:

1. After specifying the parameters for the operation, click [Save As].

2. Click [Download] to display the File Download dialog.

3. Click [Save] then save the file to the local machine— that is, the machine where the browser is running—or network location of your choice.

   TIP: You may want to change the default file name to one that is more unique and descriptive.

4. When the file has finished saving, click [Close] to dismiss the open dialogs.

Modifying Instructions

Depending on the operation, you may be able to modify some or all of the parameters of XML Instructions with valid values. For example, while the Migrate User action only permits one user to be migrated via the ControlPoint application interface, you can run the operation on multiple users by adding them to the XML instructions.
You should not attempt to change any part of the instructions apart from modifiable parameters. It is strongly recommended that you make a copy of the XML file before editing it, as it is possible that unintended changes can be made to tags or unmodifiable portions of the file.

```xml
<Operation Type="Action" Codes="MigrateUser">
  <Selectors>
    <selector>
      <item name="2007SHAREPOINT (Home Farm)" type="FARM" guid="efce6a5-627d-4f44-b503-7e83ff6b9b29" id="0" parentid="1" AllChildren="True" action="none"/>
      <item name="http://2008sharepoint1919/"/>
      <item name="Farm\Config\FARMGUID=efce6a5-42d7-4f44-b503-7e83ff6b9b29,FARMNAME=0\SharePoint_Config\FarmTool\"/>
    </selector>
  </Selectors>
  <migrateUser>
    <item>
      <key>
        <string>AXCELERTEST\samuelecilem</string>
      </key>
      <value>
        <string>AXCELERTEST\marktwain</string>
      </value>
    </item>
    <item>
      <key>
        <string>AXCELERTEST\stephendalas</string>
      </key>
      <value>
        <string>AXCELERTEST\jamesjoyce</string>
      </value>
    </item>
    <item>
      <key>
        <string>AXCELERTEST\marysmith</string>
      </key>
      <value>
        <string>AXCELERTEST\maryjones</string>
      </value>
    </item>
  </migrateUser>
  <Warnings />
  <ScheduledCurrentUser />
</Operation>
```

Executing Instructions

To execute Instructions for a ControlPoint operation:

1. Use one of the following options:
   - From the SharePoint Hierarchy select the farm node, then from the context menu or ribbon Home tab choose Execute Saved Instructions.
From the Manage ControlPoint panel, choose **Execute Saved Instructions**.

2 Click **[Browse...]** and locate the **XML File** with the instructions you want to execute.

3 Click **[Upload]**.

Now you can either:

- run the operation immediately (by clicking the **[Run Now]** button)

OR

- **schedule the operation to run at a later time.**
Analyzing SharePoint Content for Compliance

If your ControlPoint license includes Compliance functionality, the ControlPoint Analyze Content feature lets you scan content for Personally Identifiable Information (PII), then specify an action to take based on the type/severity of the information found.

Compliance Functionality Process Overview

The process for using Metalogix Sensitive Content Manager to implement ControlPoint Compliance functionality is described below.

A. ControlPoint Application Administrator registers with Metalogix Cloud Services using the credentials supplied by your Metalogix Account Manager.

B. ControlPoint Compliance Administrators define Compliance Action Rules.

C. ControlPoint Compliance Administrators submit content to Metalogix Sensitive Content Manager for analysis.

D. ControlPoint Compliance Administrators manage Compliance Actions.
Compliance Administrators and Quarantine Administrators Groups

If your organization is licensed for Compliance functionality, only individuals who have been added to the following group(s) in the ControlPoint Configuration Site will be permitted to perform Compliance actions:

- ControlPoint Compliance Administrators - Individuals permitted to access ControlPoint Compliance functionality.
- ControlPoint Quarantine Administrators - Individuals permitted to manage quarantined content.

Registering with Metalogix Cloud Services

The first time a member of the Compliance Administrators group invokes ControlPoint Compliance functionality, that user will be prompted to register with Metalogix Cloud Services. Your Metalogix Account Manager can provide this information.

Once it has been registered, all members of the ControlPoint Compliance Administrators group can begin to use ControlPoint Compliance functionality.

Compliance Action Severity Levels

When content is analyzed by the Metalogix Sensitive Content Manager, it is evaluated against the following three severity levels:

- Severe
- Moderate
• Mild

Compliance Administrators specify the appropriate action to take for each severity level via the ControlPoint Compliance Actions page.

By default, the first time scan results are returned from Metalogix Content Sensitive Manager for a particular list or library, ControlPoint creates a metadata column in that list or library called Scan Result. The classification returned for each item scanned is recorded in this column.

![Metadata Column Example]

NOTE: ControlPoint Application Administrators can prevent this column from being added by changing the ControlPoint Setting Add Scan Results Column to Scanned SharePoint List (AutomaticComplianceUpdate). See the ControlPoint Administration Guide for details.

Defining Compliance Action Rules

Members of the ControlPoint Compliance Administrators group can define Compliance Action rules to determine how non-compliant content should be handled, based on the severity level detected. You can also specify that one or more users be alerted via email when a Compliance Action is taken.

REMINDER: Your organization must be registered with Metalogix Cloud Services and you must be a member of the ControlPoint Compliance Administrators group to use this functionality.

To access the Compliance Actions page:

Use the information in the following table to determine the appropriate action to take.

<table>
<thead>
<tr>
<th>If you are creating ...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>a global set of rules independent of a particular scan job</td>
<td>from the Manage ControlPoint tree, choose ControlPoint Configuration &gt; Compliance Actions.</td>
</tr>
</tbody>
</table>
| a set of rules for a specific scan job that has been returned from Metalogix Cloud Services | • From the Compliance Summary page, select the scan job to which you want to apply the rule.  
• Click [Apply Compliance Actions]. |

To define Compliance Action rules:

1. Enter a unique name to create a new Compliance Action, or choose an existing action from the drop-down.
CONTROLPOINT COMPLIANCE ACTIONS
Create downstream Security Actions that occur upon scanning of sensitive content.

Enter a unique name to create a new compliance action. You may also edit an existing compliance action.

Employee Records

WARNING: If you choose to Update Existing Compliance Actions, the changes will be applied to all scan jobs that use it going forward. This is especially noteworthy in the case of ControlPoint policies, because once the policy is created the most current definition of the Compliance Actions is applied automatically based on scan results.

2 For each of the Severity levels (Mild, Moderate, and Severe), specify the action that should be applied when a threat is detected. You can choose to have ControlPoint:

- Take No Action on non-compliant content
- Quarantine non-compliant content
- Use an Approval Workflow to address non-compliant content
- Remove non-compliant content

Note that an action must be defined for all three severity levels. You can navigate from one rule to the next via the Select actions for threat level: button.

3 If you want ControlPoint to send an email alert when a specified action is taken:

a) Check the Alert Users box.

b) Click [Create New User].

c) Complete the Select Users for the user to which you want to send the alert.

NOTE: Currently, you can only select one user at a time. Repeat substeps b) and c) for each user you want to alert.
If you have chosen to have ControlPoint Quarantine an item with non-compliant content, you can also choose to have an alert sent to all members of the ControlPoint Quarantine Administrators group.

- Quarantine
- Alert ControlPoint Quarantine Administrators

If you have chosen to use an Approval Workflow, follow the instructions for “Using an Approval Workflow,” following.

4 When you have finished defining Compliance Rules for each Severity Level, click [Save].

**Using An Approval Workflow**

If you have chosen to use an Approval Workflow to address non-compliant content, after clicking the [Create New User] button:

1 First, select the user who will be notified by ControlPoint to start the workflow when non-compliant content is found

2 Select additional users who will be designated as approvers.

![Select Users]

**NOTE:** The user you select to start the workflow must have permissions to Edit Items and approvers must have permissions to Approve Items for lists within the scope of the Compliance Action.

You can also choose to have SharePoint notify approvers

- One at a Time (Serial)
OR

- All At Once (Parallel)

3 Click [Add User].

4 If you want SharePoint to notify additional users when an approval workflow starts and ends:
   a) Click [Create New User].
   b) Select the users you want to notify.
   c) Choose Notify these people when the workflow starts and ends without assigning tasks to them.
   d) Click [Add User].

5 For Request, enter the message that you want to be sent to users with assigned tasks.

Compliance Action Alert Email

When a Compliance Action rule includes an alert, an email, which identifies the Severity Level and action taken, is automatically sent to selected recipients.

ControlPoint Application Administrators can change the default text for the email by updating the applicable ControlPoint Configuration Setting:

- ComplianceMildLevelThreatsEmailBody
- ComplianceModerateLevelThreatsEmailBody
- ComplianceSeverLevelThreatsEmailBody

Refer to the ControlPoint Administrators Guide for details.
Submitting Content to Metalogix Sensitive Content Manager for Compliance Analysis

Members of the ControlPoint Compliance Administrators group can use the ControlPoint Analyze Content action to submit content to the Metalogix Sensitive Content Manager where it will be scanned for Personal Identifiable Information (PII). ControlPoint submits the following types of content for scanning:

- files within Document Libraries with the following extensions:
  - .doc
  - .docx
  - .msg
  - .pdf
  - .pps
  - .ppt
  - .xls
  - .xlsx
  - .txt
- items within most types of lists (with or without attachments that have any of the file extensions listed above).

NOTE: If a ControlPoint Policy has been created to “Scan item for sensitive data...” content will automatically be submitted when the policy is triggered.

To submit content to the Metalogix Sensitive Content Manager for analysis:

1. Select the object(s) containing the items that you want to submit for analysis.
2. Choose Compliance > Analyze Content.
   
   REMINDER: Your organization must be registered with Metalogix Cloud Services and you must be a member of the ControlPoint Compliance Administrators group to use this functionality.
3. Enter a name and description for the scan.
If you want to Resubmit files that have not changed since they were previously scanned, check this box.

NOTE: If you leave this box unchecked, previously-scanned files that have not changed will be excluded.

Include one or more list types from the list box. (If you also want to Include attachments, check this box.)

Now you can either:

- run the operation immediately (by clicking the [Analyze Now] button)

OR

- schedule the operation to run at a later time.

OR

- save the operation as XML Instructions that can be executed at a later time.

Ongoing and recent scan jobs display in the grid in the bottom half of the page. You can link to the Compliance Summary page for a particular scan job by clicking the View Report link.

Managing Compliance Actions

Members of the ControlPoint Compliance Administrators group can view and take action on Content Analysis scan job results returned by the Metalogix Sensitive Content Manager via the Compliance
Summary page. You can:

- view the details of a Compliance Action job
- apply Compliance Actions
- view detailed information about scan results for individual items
- if you are also a member of the ControlPoint Quarantine Administrators group, manage quarantined items
- reclassify items that returned from Metalogix Sensitive Content Manager with a status of "Unable to Classify"
- save items of a particular severity level as a selection that can be used to perform ControlPoint operations.

To manage Compliance Action scan results:

1. Select the object(s) containing the scan jobs you want to view/edit.

   NOTE: You can also access this page from the Analyze Content page, via the Page View link for a specific job.

2. If you want to view jobs for a different date range, change the Start and/or End dates and click [Find Scan Jobs].

3. Select the type of scan jobs you want to view/edit. Use the information in the following table for guidance.

<table>
<thead>
<tr>
<th>If you want to view ...</th>
<th>Select ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>all jobs submitted to Metalogix Sensitive Content Manager via the ControlPoint Analyze Content action, regardless of whether Compliance Actions were applied</td>
<td>Real time scans.</td>
</tr>
<tr>
<td>all jobs for which Compliance Actions have been applied</td>
<td>Compliance Action jobs.</td>
</tr>
</tbody>
</table>

4. Click [Find scan jobs].

5. Select the job whose details you want to view.

The following details about the selected job display beneath the grid:

- Classification Result Counts - The number of items that fall into each classification
- Scan Information - Description of and metrics associated with the job itself
- Scan Results Summary - A pie chart that shows the distribution of items among classifications.
Acting on Compliance Analysis Results

Use the information in the following table to determine the appropriate action to take.

NOTE: Any option that is not valid for the result set is not available for selection. For example, if you are viewing Compliance Action jobs, the option to Apply Compliance Actions will be disabled.

<table>
<thead>
<tr>
<th>If you want to ...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>view more detailed information about scan results for individual items (and, optionally, export results for closer analysis)</td>
<td>click [View Detailed Classification Analysis].</td>
</tr>
</tbody>
</table>

Note that there is a separate tab for each classification, with detail about each item for which scan results were returned.
<table>
<thead>
<tr>
<th><strong>If you want to ...</strong></th>
<th><strong>Then ...</strong></th>
</tr>
</thead>
</table>
| If you want to download a tabs-worth of results: | a) Choose one of the following export formats:  
  - XLS format (for opening in a pre-2007 version of Excel)  
  - Excel XML format (for opening in Excel 2007 or later)  
  - PDF formal  
  b) Click **[Export]**. |
| re-classify an item that returned "Unable to Classify" | see **Reclassifying Items Returned as Unable to Classify**.  
  If you want an action to be taken on any items that were returned by Metalogix Sensitive Content Manager as 'Unable to Classify,' you must reclassify them before applying Compliance Actions to the scan job. |
| manage quarantined items (and you are a member of the ControlPoint Quarantine Administrators group) | see **Managing Quarantined Items**. |
| apply Compliance Actions to the selected job | a) Click **[Apply Compliance Actions]**.  
  **NOTE:** This option is not available if you filtered results by Compliance Action Jobs.  
  b) Either:  
  - select a previously-defined Compliance Action from the drop-down OR  
  - define a new Compliance Action.  
  **WARNING:** If you choose to Update Existing Compliance Actions, the changes will be applied to all scan jobs that use it going forward. This is especially noteworthy in the case of ControlPoint Policies, because once the policy is created the most current definition of the Compliance Actions is applied automatically based on scan results. |
<table>
<thead>
<tr>
<th>If you want to ...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>view items for which Compliance Actions have been taken</td>
<td>c) When finished, click [Apply actions to current scan].</td>
</tr>
</tbody>
</table>
| download items of a particular severity level (Mild, Moderate, or Severe) as a reusable selection on which you can perform ControlPoint operations | a) From the drop-down to the right of the icon, select a Classification (Severity Level).  
   b) Click [Get Selection]. |

Note that there is a separate tab for each action taken, with a list of items and the associated classifications returned by Metalogix Cloud Services.

If you want to download a tabs-worth of results:

a) Choose one of the following export formats:
   - XLS format (for opening in a pre-2007 version of Excel)
   - Excel XML format (for opening in Excel 2007 or later)
   - PDF format
b) Click [Export].
Reclassifying Items Returned as Unable to Classify

If an item is returned from Metalogix Sensitive Content Manager with a Classification of 'Unable to Classify,' it means that the service detected "probable" PII but was unable to classify it definitively as PII. You can, however, review the file and apply a classification manually before applying a Compliance Action to the scan job.

If you want an action to be taken on any items that were returned by Metalogix Sensitive Content Manager as 'Unable to Classify,' you must reclassify them before applying Compliance Actions to the scan job.

To reclassify items returned as 'Unable to Classify':

1. From the Detailed Security Classification Analysis page, select the Unable to Classify tab.
2. Select the item(s) to which you want to apply a particular classification.
3. Select a classification from the drop-down, then click [Reclassify].

NOTE: If you want to review the contents of an item before assigning a classification, click the URL link to open the item.
You will be prompted to confirm the action before continuing.

CAUTION: Once you reclassify an item, the drop-down becomes disabled and the item cannot be reclassified again. If Compliance Actions have already been applied to the scan job containing the item(s), the Reclassify option will no longer appear on the page.

Once an item has been reclassified:

- it will be moved to the appropriate tab for the classification

AND

- the classification change(s) will be reflected on the Compliance Summary page.

Managing Quarantined Items

If you are a member of the ControlPoint Quarantine Administrators group, you can manage items that have been quarantined as a result of a Compliance Action. When an item is quarantined, it remains in the same location in the SharePoint list, but all permissions—except those of ControlPoint Quarantine Administrators—are removed.

To manage quarantined items:

1. Use the information in the following table to determine the appropriate action to take.

<table>
<thead>
<tr>
<th>If you are starting from ...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>the SharePoint Hierarchy</td>
<td>a) Select the object(s) containing the quarantined items you want to manage.</td>
</tr>
<tr>
<td></td>
<td>b) Choose Compliance &gt; Manage Quarantined Items.</td>
</tr>
<tr>
<td>the Compliance Summary page</td>
<td>a) Make sure the Compliance Action jobs radio button is selected.</td>
</tr>
<tr>
<td></td>
<td>b) Select the Scan job containing the quarantined items you want to manage.</td>
</tr>
<tr>
<td></td>
<td>c) Click [Manage Quarantined Items].</td>
</tr>
</tbody>
</table>
2. Select the quarantined item(s) you want to act on.

3. If you want to review the content of a quarantined item before taking an action, click the Document link in the View column.

Now you can either:

- remove the item from quarantine
  
  **NOTE:** When you remove an item from quarantine, it is restored in its original location with the same permissions it had before it was quarantined.

  OR

- permanently delete the file(s).

### Reporting on Sensitive Content Activity

If you are a member of the ControlPoint Compliance Administrators group, you can use the ControlPoint Sensitive Document Activity report to view detailed information about documents analyzed by Content Sensitive Manager that:

- have been identified as "sensitive content" (that is, have been assigned a Severity Level)
  
  AND

- have been accessed by at least one SharePoint user.

### Before you can report sensitive document activity:

- Auditing must be enabled for each list or library for which you want to report sensitive document activity. You can enable these settings for individual site collections from within SharePoint.

- At least one Compliance scan must have been returned by Sensitive Content Manager with items
that have been assigned a **Severity Level**.

**To report sensitive document activity:**

1. **Select the object(s) for which you want to report sensitive document activity.**
2. Choose **Compliance > Sensitive Document Activity**.

The tiles at the top of the report highlight the following statistics for the selected time period (by default, the past month):

- **Total Number of SCM (Content Sensitive Manager) Classified Documents**
- **Sensitive Documents Accessed** (that is, the *number of times* a document identified as sensitive content has been accessed by a SharePoint user)
- **Users Accessing Sensitive Documents** (that is, the *number of unique SharePoint users* who have accessed documents identified as containing sensitive content)
- **Realtime Scanning** (that is, the number of days since the last [realtime scan](#) was performed)

**To filter results that display in the body of the report:**

1. Choose a different severity level from the **Filter** drop-down and/or modify the default date range.
2. Click [Refresh].

**Graph Tab**

The Sensitive Document Activity report **Graph** tab illustrates the Activity Count by Sensitivity for the selected Severity Level(s) and date range.

Note that you can click a Severity Level in the legend at the right side of the page to hide/display it.

**Files Tab**

The Sensitive Document Activity report **Files** tab lists all of the documents the Content Sensitive Manager identified as "sensitive content" for the selected Severity Level(s), grouped by list or library.

Note that this tab displays *all* content sensitive classified documents for the selected Severity Level(s), regardless of whether they have been accessed, and the date range filter does *not* apply.
Users Tab

The Users tab lists the SharePoint users who have accessed documents with sensitive content within the specified time period, along with the Number of Docs Accessed.

Activity Tab

The Activity tab lists each individual instance of sensitive content activity, including the User Name, Activity Type, document Severity Level and Activity Date.
Using ControlPoint Sentinel to Detect Anomalous Activity

ControlPoint Sentinel functionality enables you to detect deviations in document views and downloads from individual users’ "typical" daily usage patterns. ControlPoint Sentinel uses the following components in its anomalous activity determinations:

- **Business Hours**: Daily start and end time for each day of the work week.
- The following **Anomalous Activity Limits**:
  - **Default daily activity limits**: The limits for each (measured in terms of document views and downloads) to apply to any user whose personal activity limits have not yet been characterized.
  - **Personal daily activity limits**: The deviation from "typical" daily usage patterns characterized for each individual user on a given day of the week.

ControlPoint Sentinel relies on SharePoint Audit Log events. Therefore, for this functionality to be effective, the auditing of Delete, Edit, and View/Download must be enabled for every site collection for which you want to collect activity data.

How Personal Daily Activity is Determined

Anomalous activity limits are set based on the statistical analysis of how often each user views and downloads documents. The personal daily activity limits used by ControlPoint Sentinel are defined in terms of standard deviations above the mean or average observed over a period of time (currently, 12 days worth of observations for each day of the week).

Standard deviation is a statistical measure of the variation within a set of data values. Two users may have the same average of document views and downloads per day, but their standard deviation or the variation in the number of documents they view and download in any given day can be very different. If a user consistently views and downloads roughly the same number of documents every day, then their standard deviation will be low. If a user is more erratic in the number of documents they view or download in a day (for example, sometimes viewing or downloading no documents, sometimes one or two, sometimes 30 or 40) then their standard deviation will be high. By using an individual user’s standard deviation to define the limits for anomalous activity the limits are tailored to each user’s usage pattern.

Using the user’s standard deviation we can determine how likely it is that a user would view or download a particular number of documents in a day. When looking for anomalous activity we are looking at activity that is not very likely, that should happen much less than 1% of the time. For highly anomalous activity we are looking for activity that should happen a very small fraction of a percentage of the time.
Defining Business Hours for Anomalous Activity Detection

The first step in Sentinel Setup is to define Business Hours, so that Anomalous Activity Limits can be defined differently for both business and non-business hours. For example, you may want to specify a lower limit for non-business hours, when typical activity is expected to be lower.

Note that Business Hours reflect the local time of the server on which SharePoint is installed.

To define business and non-business hours for anomalous activity detection:

1. From the Manage ControlPoint tree choose ControlPoint Sentinel > Sentinel Setup.
2. On the Sentinel Setup page, make sure the Business Hours tab is selected.
3. For each day that you want activity data to be collected, select the start and end time that represent the standard work hours for that particular day, and make sure the Work Day box is checked.
4 For each non-work day, uncheck the Work Day box.

<table>
<thead>
<tr>
<th>Day</th>
<th>Start Time</th>
<th>End Time</th>
<th>Work Day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Saturday</td>
<td>12:00 AM</td>
<td>12:00 AM</td>
<td></td>
</tr>
<tr>
<td>Sunday</td>
<td>12:00 AM</td>
<td>12:00 AM</td>
<td>Work Day</td>
</tr>
</tbody>
</table>

NOTE: When the Work Day box is unchecked, activity data will not be collected for that day. Start and end times are irrelevant and will be cleared when you save the setup.

5 When you have finished defining business and non-business hours, click [Save Setup].

Defining Base Line Rules for Anomalous Activity Detection

You can define two types of anomalous activity limits:

- Default daily activities, which are used for all users until personal user limits have been characterized.
- Personal daily activities, which are used as soon as a user’s personal activity limits have been characterized.

NOTE: For each day of the week, personal user limits replace default daily limits after 12 days worth of observations by the Anomalous Activity Detection Job.

To access the Anomalous Activity Limits page:

From the Sentinel Setup page, select the Anomalous Activity Limits tab.

Defining Default Daily Activity Limits

Default Daily Activity Limits are expressed in terms of the number of “typical” views and downloads. Because they apply to all users until personal user limits have been characterized, it is recommended
that you enter limits that would be considered typical and anomalous for any SharePoint user in your organization. For example, 100 document views and downloads per day may take into account “typical” daily activity for your most active users without being an alarmingly high number for less active users. Double that number may be considered moderately anomalous, while triple that number may be considered highly anomalous.

Default daily activity limits:
The default daily activity limits used for all users until personal user limits have been characterized.

<table>
<thead>
<tr>
<th>Limit Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Typical daily activity limit</td>
<td>100</td>
</tr>
<tr>
<td>Moderately anomalous activity limit</td>
<td>200</td>
</tr>
<tr>
<td>Highly anomalous activity limit</td>
<td>300</td>
</tr>
</tbody>
</table>

Document views and downloads

NOTE: If you do not want ControlPoint Sentinel to track Default Daily Activity Limits, leave the limit fields set to 0.

Defining Personal Daily Activity Limits

The following table shows the percentage of values that fall around or above the mean in terms of the standard deviation.

<table>
<thead>
<tr>
<th>Standard Deviations (σ) Above the Mean</th>
<th>Percentage (%) of Values Above the Standard Deviations from the Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>1σ</td>
<td>15.86553%</td>
</tr>
<tr>
<td>2σ</td>
<td>2.275013%</td>
</tr>
<tr>
<td>3σ</td>
<td>0.13499%</td>
</tr>
<tr>
<td>4σ</td>
<td>0.003167%</td>
</tr>
<tr>
<td>5σ</td>
<td>0.000028665%</td>
</tr>
<tr>
<td>6σ</td>
<td>0.0000009865%</td>
</tr>
<tr>
<td>7σ</td>
<td>0.0000000128%</td>
</tr>
</tbody>
</table>

It is recommended that you:

- Set the Typical daily activity limit to 3 standard deviations above the mean.
  A user could exceed this limit once every two years. This is not cause for concern but if it happens more frequently than that it may warrant investigation.

- Set the Moderately anomalous activity limit to 5 standard deviations above the mean.
  A user could exceed this limit once in about 10,000 years. This is an indication of anomalous activity that should be investigated immediately.

- Set the Highly anomalous activity limit to 7 standard deviations above the mean.
This level of activity is very very unlikely and should be acted upon immediately.

**Personal daily activity limits:**
The personal daily activity limits are based on the historical analysis of each user's typical activity. The personal limits will be used once enough information has been gathered about a user's typical usage.

Limits are defined as number of standard deviations above the average daily document views and downloads for a given user.

- Typical daily activity limit: 3 standard deviations
- Moderately anomalous activity limit: 5 standard deviations
- Highly anomalous activity limit: 7 standard deviations

See also [How Personal Daily Activity is Determined](#).

### Defining Anomalous Activity Rules

After you have defined Business Hours and Activity Limits, the next step is to define Anomalous Activity Rules, or the action (if any) to take when a defined activity limit is exceeded, during both business hours and non-business hours.

**To define Anomalous Activity Rules:**

1. From the Sentinel Setup page, select the Anomalous Activity Rules tab.
2. If you want to have an alert generated whenever a limit is exceeded for a particular combination of criteria (Business Hours/Non-Business Hours; Default Daily Activity/Personal Activity; Activity Limit):
   - Select Alert from the Action drop-down.
   - If you want to have an email generated when the limit is exceeded, enter an Email address. (You can enter multiple email addresses, separated by commas (,).

   **NOTE:** Only limits to which an Alert is applied will be subject to Sentinel reporting. Limits with No Action Required will not be reported.

### Preparing Your Environment for Using ControlPoint Sentinel

Before ControlPoint Sentinel can begin collecting data for Anomalous Activity Detection:

A. SharePoint auditing must be enabled on all site collections for which Anomalous Activity detection will be performed.

B. Anomalous Activity Detection must be enabled to run:
   - via the ControlPoint Anomalous Activity Detection job
   - OR
- as part of the ControlPoint **Scheduler Job**.

**Enabling SharePoint Auditing**

ControlPoint Sentinel analyzes the following SharePoint audit log events for Anomalous Activity Detection:

- Editing items
- Deleting items
- Opening or downloading documents, viewing items in lists, or viewing item properties.

You can enable these settings for individual site collections from within SharePoint.

**Enabling the Anomalous Activity Detection Job**

1. From the Manage ControlPoint tree choose Schedule Management and Logging > Schedule Monitor.
2. Choose **Switch Monitor Views** > Windows Jobs.
3. Click the Edit icon (📝) to the left of the AnomalousActivityDetectionJob.
4. Check the **Active** box.
By default, the job is scheduled to run daily, at 4:00 am (local server time). You may however, change the schedule to run more frequently. Note that, the more frequently the job is run, the sooner an alert may be generated when an Anomalous Activity Limit is reached.

**Enabling Anomalous Activity Detection via the ControlPoint Scheduled Job Review**

As an alternative to using the Anomalous Activity Detection Job, you can choose to have anomalous activity detection performed as part of the ControlPoint **Scheduler Job** (which, by default, runs every 10 minutes). ControlPoint Application Administrators can enable this option by changing the ControlPoint Configuration Setting **Enable Options That Require Anomalous Activity Detection** from **False** to **True**.
Refer to the ControlPoint Administration Guide for more detail on modifying ControlPoint Configuration Settings.

**Reporting Anomalous Activity**

The ControlPoint Sentinel Report lets you view anomalous activity events for which an Alert has been specified on the Sentinel Setup - Anomalous Activity Rules page. You can also filter results by user and/or date range.

**To report anomalous activity:**

1. From the Manage ControlPoint tree choose ControlPoint Sentinel > Sentinel Report.
2. If you want to narrow your results, enter one or more user(s) in the People Picker and/or enter a date range.

**NOTE:** If you leave the From and To Dates blank, all available results will be returned.

The tiles at the top of the report highlight the following statistics:

- The **Total Number of Anomalous Activities Detected**
- The number of **High Risk Events** as characterized by ControlPoint Sentinel
- The **Number of Users** with anomalous activity
- The **Security Risk Score** (which is derived by the Severity of each activity within the date range covered by the report)

For each anomalous event detected, report detail displays:

- the **Event Time** (that is, the date and the time when the ControlPoint Anomalous Activity Detection Job captured the event)
- the **User** whose activity triggered the anomalous activity detection alert
- the **Event Severity** (as defined on the Sentinel Setup - Anomalous Activity Limits page)
- the **Triggering Activity Level** that resulted in the anomalous activity detection alert:
• for **Default** daily activity, activity above the specified limit for the Event Severity

• for **Personal** daily activity, the amount of activity for the Event Severity to which the specified deviations above from the user’s “typical” usage pattern have been applied.

• the **Expected Activity Level**:

  • for **Default** daily activity, the specified limit for the Event Severity
  
  • for **Personal** daily activity, "typical" usage pattern as calculated by ControlPoint Sentinel

• the **Delta Activity Level** (that is, the difference between Triggering Activity Level and the Expected Activity Level).

**To view detailed audit log data for a user:**

Click the User link to generate a ControlPoint Audit Log analysis.