DocAve® 6 Administrator

User Guide

Service Pack 4

Revision L

Issued May 2014

The Enterprise-Class **Management Platform** for **SharePoint®** Governance

Table of Contents

DocAve 6: Administrator

About DocAve Administrator for SharePoint

As deployments expand and evolve, organizations must find ways to enforce governance policies, control site sprawl, and easily view and edit permissions across entire Microsoft SharePoint 2010 or SharePoint 2013 environments. DocAve Administrator for SharePoint gives organizations the agility and control they require to easily meet these critical management Administrator for SharePoint challenges. Perform tasks on a single farm or hundreds of farms to ensure that SharePoint fulfills your specific business needs.

- From a single interface, view, search, manage, report on, deploy, and replicate configurations, securities, and content across all SharePoint assets.
- Maintain compliance with SharePoint governance policies for SharePoint content, configurations, and customizations for enhanced lifecycle management.
- Apply the same level of administration and replication to all content externalized with DocAve's RBS provider.

Complementary Products

Many products and product suites on the DocAve 6 platform work in conjunction with one another. The following products are recommended for use with Administrator for SharePoint:

- DocAve Content Manager for SharePoint for restructuring or moving SharePoint content
- DocAve Report Center for SharePoint to examine pain points in the SharePoint infrastructure and report on SharePoint user behavior and changes
- DocAve Data Protection for setting backup and recovery points prior to adjusting SharePoint governance policies in this product

Submitting Documentation Feedback to AvePoint

AvePoint encourages customers to provide feedback regarding our product documentation. You can Submit Your Feedback on our website.

Before You Begin

Refer to the sections for system and farm requirements that must be in place prior to installing and using DocAve Administrator for SharePoint.

Configuration

In order to use DocAve Administrator for SharePoint (hereafter referred to as Administrator), the DocAve 6 platform must be installed and configured properly on your farm. Administrator will not function without DocAve 6 present on the farm. For installation instructions, see the DocAve 6 Installation Guide.

Agents

DocAve Agents are responsible for running DocAve jobs and interacting with the SharePoint object model. DocAve Agents enable DocAve Manager to communicate with the respective servers, allowing for Administrator commands to function properly.

*Note: The use of system resources on a server increases when the installed Agent is performing actions. This may affect server performance. However, if the Agent installed on a server is not being used, the use of system resources is very low and, therefore, the effect on server performance is negligible.

For instructions on installing the DocAve Platform, DocAve Manager, and DocAve Agents, see the DocAve 6 Installation Guide.

Required Permissions

Refer to the section below for the required permissions for installing and using DocAve Administrator on SharePoint on-premises and SharePoint Online environments.

Administrator for SharePoint On-Premises Permissions

To install and use Administrator for SharePoint on the SharePoint on-premises environment properly, ensure that the Agent account has the following permissions:

1. Local System Permissions: These permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.

2. SharePoint Permissions: These permissions must be manually configured prior to using DocAve 6 Administrator; they are not automatically configured.

- User is a member of the **Farm Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.

- Full Control to all zones of all Web applications via User Policy for Web applications.

- Full Control to the User Profile Service Application related to the Web application where the personal site resides.

2. SQL Permissions: These permissions must be manually configured prior to using DocAve 6 Administrator; they are not automatically configured.

- Member has a Database Role of **db_owner** for all the databases related to SharePoint, including Content Databases, Config Database, and Central Admin Database.

- Server Role of **dbcreator** and **securityadmin** in SQL Server.

Administrator for SharePoint Online Permissions

To install and use Administrator on the SharePoint Online environment properly, the Agent account and the account specified when adding the SharePoint Online or on-premises site collections to SharePoint Sites Group has the following permissions:

1. Agent account permissions:

- Local System Permissions: The permissions are automatically configured by DocAve during the installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.

   *Note: If the registered site collections are SharePoint Online site collections, the Agent account is on the Agent machine that has network connection or has configured **Agent Proxy Settings** before registering SharePoint Online site collections.

   If the registered site collections are on-premises site collections, the Agent account is on the Agent machine that will run the Administrator job.

2. Site Collection user permissions:

- Member of the **Site Collection Administrators** group of each site collection where you want to use Administrator Migration.

- Managed Metadata Service

   o Term Store Administrator

   *Note: If using the **Scan Mode** to add the site collections to the SharePoint Sites Group in Control Panel, make sure that the Office 365 account has the **Global Administrator** permission

in the specific SharePoint admin center site or the SharePoint account has the Full Control permission for All Zones in the Web application where the site collections reside.

Local System Permissions

The following Local System Permissions are automatically configured during DocAve 6 installation:

- User is a member of the following local groups:
    - IIS WPG (for IIS 6.0) or IIS IUSRS (for IIS 7.0)
    - Performance Monitor Users
    - DocAve Users (the group is created by DocAve automatically; it has the following permissions):
        - Full Control to the Registry of HKEY LOCAL MACHINE\SOFTWARE\AvePoint\DocAve6
        - Full Control to the Registry of HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\eventlog6
        - Full Control to the Communication Certificate
        - Permission of Log on as a batch job (it can be found within Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > User Rights Assignment)
        - Full Control Permission for DocAve Agent installation directory
    - Local admin permission

Getting Started

SharePoint and the DocAve platform modules have common functionality. While some of this shared functionality is covered in this guide, the primary focus of this document is the functionality that is specific to the DocAve module.

For information on the shared functionality not covered in this document, refer to SharePoint Help. To view tables presenting operations that are shared between DocAve and SharePoint at various levels, refer to Appendix B: DocAve Administrator and SharePoint Operations.

Refer to the sections below for important information on getting started with Administrator.

Launching Administrator for SharePoint

To launch Administrator and access its functionality, complete the following steps:

1. Log in to DocAve. If you are already in the software, click the **DocAve** tab. The **DocAve** tab displays all modules on the left side of the window.

2. From the **DocAve** tab, click **Administration** to view the Administration functions.

3. Click **Administrator** to launch Administrator for SharePoint.
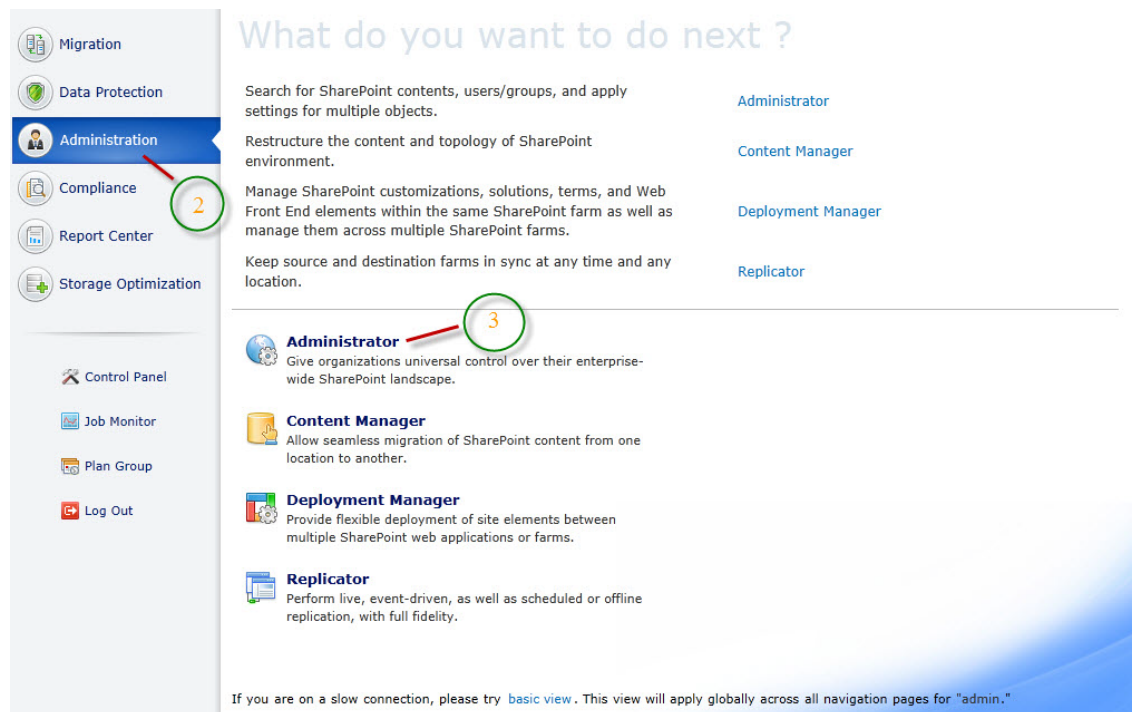
Figure 1: DocAve module launch window.

User Interface Overview

The Administrator user interface launches with the **Management** tab active. This tab displays your farm environment and allows for quick access to a list of Administrator features.
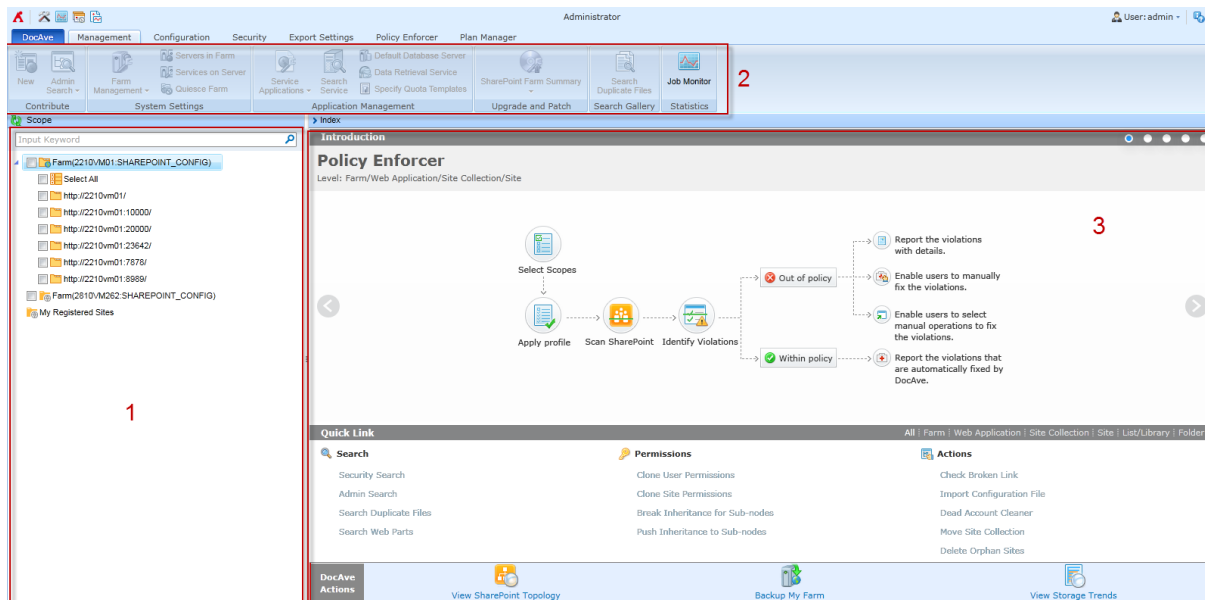
Figure 2: Administrator landing page.

1. The **SharePoint tree** (**Scope** panel) displays all content within your farms. Use this panel to select the content that you wish to perform actions on. Selecting content often reveals new tabs and functionality on the **ribbon**.

2. The **ribbon** shows the available actions and wizards for the selected nodes. This content is dynamic; it will often change depending on what is selected in the SharePoint tree.

3. The **workspace** shows all form-based content that is used during the configuration of actions performed in DocAve products.

Selecting Farms and Nodes

To select farms and nodes, complete the following steps:

1. From the **Scope** panel on the left, click the farm that contains the relevant SharePoint content. You can input a keyword into the Search box above the farm tree to filter out the relevant SharePoint content.

2. Select the relevant content from which you want to perform further operations by clicking the checkboxes to the left of the content.

3. After selecting content, you will be able to perform the procedures described throughout this guide.

*Note: Nodes on different SharePoint farms cannot be selected at the same time. SharePoint Online site collections in both SharePoint 2010 and 2013 will be displayed in a SharePoint Online farm.

*Note: Use Security Trimming to limit which objects specific users can see when browsing the farm tree. Security Trimming allows the user to view the site collections on the tree for which the user is a SharePoint user. This allows the user to expand the corresponding site collection node and perform actions on all the SharePoint objects inside it. However, the user cannot perform actions at the Web application and farm levels. For details on configuring a SharePoint site with Security Trimming, refer to the [DocAve 6 Control Panel Reference Guide](#).

Previewing Files in SharePoint Using the DocAve Preview Feature

DocAve provides a solution named **SP2013PreviewGUI.wsp** for SharePoint 2013 and **SP2010PreviewGUI.wsp** for SharePoint 2010 to add a feature named **DocAve Preview** to site collections in your SharePoint environments. This feature allows you to preview library files in image format, without requiring any local software installation for those files.

*Note: The DocAve Preview feature is supported for Office files, PDF files, CAD files, and pictures in all of the out-of-box SharePoint libraries and Connector libraries.

Deploying the DocAve Preview Solution

To use the DocAve Preview feature in SharePoint, you must first deploy the **SP2013PreviewGUI.wsp** to your SharePoint 2013 farm or **SP2010PreviewGUI.wsp** to your SharePoint 2010 farm. Once you have installed and deployed the solution, the **DocAve Preview** feature will be listed in the **Site Collection Features** List.

*Note: To deploy this solution, each Web front-end server must have DocAve Agent installed.

To deploy the DocAve Preview Solution to your SharePoint 2013 farm, complete the following steps:

1. Navigate to: **DocAve** > **Control Panel** > **Solution Manager**.
2. Select the target farm from the **Farm** drop-down list.
3. Check the **SP2013PreviewGUI.wsp** checkbox.
4. Click **Install** in the **Actions** group on the ribbon. Once the solution is installed on the SharePoint farm, the following message will appear in the **Message** column: **Installed the solution successfully**.
5. Check the **SP2013PreviewGUI.wsp** checkbox again.
6. Click **Deploy** in the **Actions** group on the ribbon. After the solution is deployed successfully. The status of the solution is shown as **Deployed** in the **Status** column.

Follow the same steps to deploy the **SP2010PreviewGUI.wsp** solution to your SharePoint 2010 farm as **SP2013PreviewGUI.wsp**.

*Note: To use the **DocAve Preview** feature in 2010 experience version site collections in a SharePoint 2013 farm, you must deploy both the **SP2010PreviewGUI.wsp** solution and the **SP2013PreviewGUI.wsp** solution to the specific SharePoint 2013 farm.

Refer to the **Solution Manager** section of the DocAve 6 Control Panel Reference Guide for more instructions on operating the solutions.

For more information on activating the DocAve Preview feature, refer to [Activating the DocAve Preview Feature](#).

Activating the DocAve Preview Feature

Once the solution is deployed, the DocAve Preview feature can be activated in SharePoint. Complete the following step to enable the DocAve Preview feature:

1. In SharePoint, access the site collection for which you want to activate the DocAve Preview feature. In SharePoint 2010, navigate to: **Site Actions** > **Site Settings** > **Site Collection features**. In SharePoint 2013, navigate to: Settings icon (⚙) > **Site Settings** > **Site Collection features**.

2. Click **Activate** next to the **DocAve Preview** feature to enable the feature for the selected site collection.

3. After activating the DocAve Preview feature, the status of the feature reads **Active** in the Status column.

Configuring the DocAve Preview Settings

After you activate the DocAve Preview feature in a particular site collection, the **DocAve Preview Settings** appears in the **Site Settings** > **Site Collection Administration** section of the site collection. Configure the **DocAve Preview Settings** to configure the cache settings for the DocAve Preview feature.

To configure the **DocAve Preview Settings**, complete the following steps:

1. In the SharePoint site collection where you have activated the feature for SharePoint 2010, navigate to: **Site Actions** > **Site Settings** > **Site Collection Administration** > **DocAve Preview Settings**. For SharePoint 2013, navigate to Settings icon (⚙) > **Site settings** > **Site Collection Administration** > **DocAve Preview Settings**.

2. In the **Enable Cache Settings** section in the **DocAve Preview Settings** page, select whether to enable cache settings for the DocAve Preview feature using the **Enable Cache** checkbox.

   - If you do not want to enable settings for the DocAve Preview feature, deselect the **Enable Cache** checkbox.

   - If you want to store copies of previewed items locally for quicker access, select the **Enable Cache** checkbox to enable the cache and initiate a SharePoint timer job named **DocAve Preview Cache Clearing Job – site collection URL**. This timer job will run scheduled jobs to check whether to clean the cache data of this site collection and then perform the retention. If you select the **Enable Cache** checkbox, configure the following settings:

     o **Cache Location** – Specify a Universal Naming Conversion (UNC) path to the location where you want to store the cache data for this feature.

   ▪ **Path** – Enter a Universal Naming Convention (UNC) path as the location where the cache data will be stored in the **UNC path** text box. For example, *\\server\c$\data*.

- **Username** – Enter the username that is available to the UNC path entered above. For example, *domain\username or username@domain.com*.

- **Password** – Enter the password for the username entered above.

  > ***Note**: The user entered for the UNC path must have **Write** or above permission to the UNC path.

  o **Cache Settings** – Enter an integer in the text box to specify how many days to save the cache data of the files that have been previewed.

  o **Schedule Settings** – Configure the schedule for the **DocAve Preview Cache Clearing Job – site collection URL** timer job to check the cache data and start the retention.

    - **Daily** – To run the **DocAve Preview Cache Clearing Job – site collection URL** timer job every day, select the **Daily** option, and then select a period using the drop-down lists during which the timer job starts to check the cache data.

    - **Weekly** – To run the **DocAve Preview Cache Clearing Job – site collection URL** timer job every week, select the **Weekly** option and then select a period using the drop-down lists during which the timer job starts to check the cache data.

    - **Monthly** – To run the retention job every month, select the **Monthly** option and then configure the **By date** or **By day** field. For detailed instructions, refer to [Advanced Start Time Settings](#).

      *Note: AvePoint does not recommend running the **DocAve Preview Cache Clearing Job – site collection URL** timer job too frequently since it would increase the burden on your SharePoint server.

3. Click **Save** to save your configurations, or click **Cancel** to cancel the configurations.

   After you save the settings, you can view the definition of the **DocAve Preview Cache Clearing Job – site collection URL** timer job by navigating to **Central Administration** > **Monitoring** > **Review Job Definition** > **Scheduled Jobs**.

Advanced Start Time Settings

If you select **Monthly** when configuring the **Schedule Settings** in **DocAve Preview Settings**, the following advanced start time settings are available:

- **By date** – If you select **By date**, configure the start time by selecting a period using the **… … on the …** drop-down lists during which the cache retention job starts to check the cache data. For example, if you select **1AM 00 on the 2nd** and **2AM 00 on the 2nd**, the **DocAve Preview Cache Clearing Job – site collection URL** timer job starts to check the data between 1 o'clock AM on the 2nd day of the month and 2 o'clock AM on the 2nd day of the month.

- **By day** – If you select **By day**, configure the start time by selecting the time on a specific day of a specific week from the **… … on the … …** drop-down lists when the **DocAve Preview Cache Clearing Job – site collection URL** timer job starts to check the cache data. For example, if you select **1AM 00 on the first Friday**, the cache retention job starts to check the data at 1 o'clock AM on the first Friday of the month.

Previewing Files in Libraries

To preview files in libraries using the DocAve Preview feature, complete the following steps:

1. Navigate to a library in the site collection where the DocAve Preview feature has been activated.

   *Note**: The DocAve Preview feature is supported for all of the out-of-box SharePoint libraries and Connector Library.

2. Select a file you want to preview by checking the corresponding checkbox.

3. Click **Preview** on the ribbon of the **Documents** tab. The preview images for the selected file appear in a pop-up window.

4. If the selected file consists of more than one page, click the arrow buttons in the bottom or on the edges of the pop-up window to view the preview image for the next or previous page of the file.

5. When you finish previewing the file, click the close (✕) button on the upper-right corner to close the pop-up window.

Viewing and Searching Content

Administrator provides an accurate and thorough search tool that uses multiple search criteria in a large scope. After performing a search, Administrator operations can be performed on multiple items in the search results.

See the topics below for information on viewing and searching for content in your farms.

Viewing Site Collection Lists

To view a list of site collections within a selected Web application, complete the following steps:

*Note: That you can only view site collection lists for one Web application at a time.

1. Select the **Scope** of the content, as described in Selecting Farms and Nodes.
2. Click the **Management** tab.
3. Navigate to a **Site Collection List** on the ribbon. The Site Collection List appears, displaying information such as **Site Collection Title**, **Database Name**, **URL**, and **Primary** Administrator. The site collection URL is linked to the corresponding SharePoint site collection; it takes you to the SharePoint site directly by clicking the site collection URL.

This functionality also exists within SharePoint 2010 and SharePoint 2013. For more information on viewing site collection lists, refer to SharePoint Help. To view tables presenting operations that are shared between DocAve and SharePoint at various levels, refer to Appendix B: DocAve Administrator and SharePoint Operations.

Viewing Users and Permissions

To view a list of user permissions for people and groups or a list of site permissions, complete the following steps:

1. Select the **Scope** of the content, as described in Selecting Farms and Nodes. This feature is supported on site collection and site levels.
2. Click **Security** > **Users and Permissions**.
3. Select either **People and Groups** or **Site Permissions**. The applicable list appears.

This functionality also exists within SharePoint 2010 and SharePoint 2013. For more information on viewing users and permissions, refer to SharePoint Help. To view tables presenting operations that are shared between DocAve and SharePoint at various levels, refer to Appendix B: DocAve Administrator and SharePoint Operations.

Performing an Admin Search using Admin Search Wizard

Admin search is useful to report on and manage all site collections, sites, lists, libraries, and items that meet given criteria (typically based on metadata, settings, or configurations). Use the Wizard for step-by-step instructions on configuring an admin search.

*Note: The list view of an Admin Search result displays a maximum of 20,000 search result nodes. Download the results to view all of the search result nodes.

To perform an admin search using the Wizard, complete the following steps:

1. Select the **Scope** of the content, as described in [Selecting Farms and Nodes](#).

2. Click **Management** > **Admin Search** > **Admin Search Wizard Mode**. The **Wizard Mode** tab appears.

3. Enter a **Plan Name** for the plan. A plan name with the format **Admin Search HH:MM:SS YYYY-MM-DD** is provided by default.

    *   Click **Check** to the plan name to check whether the specified plan name is available. A green check mark indicates that the specified plan name is available. A warning message appears if the specified plan name already exists and some suggested plan names are listed beneath.

    *   Add an optional **Description** if desired.

4. Click **Next** on the ribbon. The **Search Filter** screen appears.

6. Use the drop-downs to add a filter rule specifying which objects or data within each SharePoint level will be searched. Click **Add** to add the rule to the list. For more information related to search filters, refer to [Appendix A: Search Filter Table](#).

    *   Change the logical relationship between two or more filter rules by clicking **And** or **Or** to the right of the list entry.

        o   **And** – The content that meets all the rules is displayed.

        o   **Or** – The content that meets one of the rules is displayed.

    *   The **Basic Filter Conditions** field lists the logical relationship between the filter rules.

    *   If desired, click the down arrow beside the filter rule number to reorder filter rules of the same level.

5. When finished setting up filter rules, click **Next** on the ribbon. The **Schedule Selection** screen appears.

6. Select a scheduling option.

    *   **No Schedule** – Select this option to run an admin search without a schedule.

    *   **Configure the Schedule Myself** – Select this option to configure a customized schedule, and run the admin search by schedule. Fill in the parameters according to your desired

schedule. After configuring the schedule for the search, click **Calendar View** to view the scheduled search by day, week, or month.

When finished configuring the schedule, click **Next** on the ribbon. The **Notification** screen appears.

7. Select a previously-created user notification profile from the **Notification** drop-down list, or select **New Notification** to configure a new user notification. Refer to the User Notification Settings section in the [DocAve 6 Control Panel Reference Guide](#) for instructions on configuring user notification.

   *Note: Click **View** to the drop-down list to view the detailed information of the selected user notification profile.

8. When finished setting up notifications, click **Next** on the ribbon. The **Overview** screen appears.

9. Review and edit the plan selections. To make changes, click **Edit** to the right of the row. This links to the corresponding setting page, allowing you to edit the configuration.

10. Click **Finish** or **Finish and Run Now** on the lower-right section of the screen. The admin search plan is now listed in Plan Manager.

Performing an Admin Search using Admin Search Form Mode

Admin Search Form Mode offers the ability to run a quick admin search by providing a truncated version of all of the Search Wizard screens on one page. Click **Management** > **Admin Search** > **Admin Search Form Mode** to access this mode For detailed information about how to configure an admin search condition, refer to [Performing an Admin Search using Admin Search Wizard](#).

*Note: If you are unfamiliar with this feature, it is not recommended that you use this search mode to run an admin search.

Performing a Security Search using Security Search Wizard

Use the wizard for step-by-step instructions on configuring a security search. To perform a security search using the wizard, complete the following steps:

1. Select the **Scope** of the content, as described in [Selecting Farms and Nodes](#).

2. Click **Security** > **Security Search** > **Security Search Wizard Mode**. The **Wizard Mode** tab appears.

3. Enter a **Plan Name** for the plan. A plan name with the format **Security Search HH:MM:SS YYYY-MM-DD** is provided by default.

   - Click **Check** to the plan name to check whether the specified plan name is available. A green check mark indicates that the specified plan name is available. A warning message appears if the specified plan name already exists and some suggested plan names are listed beneath.

- Add an optional **Description** if desired.

4. Click **Next** on the ribbon. The **Permissions** screen appears.

5. Enter the **User and Group** for which to search. Click the **Check Names** icon to verify the inputted names, or click the **Browse** icon to browse through a list of names.

   *Note: If no users or groups are specified in the **User and Group** field, all of the users or groups under the specified nodes are searched.

6. Click **Advanced Settings** to specify the relevant search conditions.

   *Note: Only the **Include SharePoint group members** option is supported for SharePoint Online sites.

   - **Search for deactivated users** – Select this box to search all the deactivated users (excluding the deactivated users with no permissions) under the selected scope and to mark the searched user with **Deleted** or **Disabled**.

   - **Include SharePoint group members** – Select this box to search all users included in the SharePoint group under the selected scope.

   - **Include Active Directory group members or Form-based Authentication role members** – Select this box to specify the search condition over complex nest relation in AD groups.
     - **All members** – Search all of the users in selected groups including its sub-groups.
     - **Limit search depth to … levels** – Limit the search depth and only search the specified levels.
     - **Exclude the following group(s)** – Enter the groups that will not be included on the search.

     For example, assume there are three AD groups: Group1, Group2, and Group3. The following is their nest relation: Group1 has a sub-group named Group2, and Group3 is a sub-group of Group2. Group1 has been added into SharePoint, while Group2 and Group3 are not. Selecting the **All members** option searches for users in Group1, Group2, and Group3. Selecting **Limit search depth to 2 levels** searches for users in Group1 and Group2, while users in Group3 cannot be searched. Selecting **Exclude the following group(s)** option and inputting Group3 into the provide field omits Group3 and its users from being searched.

7. Configure the **Permission Settings** to limit the users or contents searched according to the permissions assigned to them.

   - **Has Permissions** – Limit the search result based upon the permission; these include **Search for Any Permission**, **Full Control**, **Design**, **Edit**, **Contribute**, **Read**, **View Only**, and **Limited Access**. After selecting the relevant permissions, click **Details** to view the detailed information of this permission.

- **Exact permission** – Match the search result with the exact permission selected, while **Exact permission or better** matches the search result with users or content whose permission is no less than the selected permission.

- **Include SharePoint users and groups with no permissions** – Select whether or not to search the SharePoint users and groups with no permissions. By default, they are excluded.

  ***Note:** Advanced options are not supported for Office 365 sites.

- **Include inherited permissions** – Select this option to include the users and groups permissions for those SharePoint objects inheriting permission settings from their parent nodes. Selecting this option will provide a result of all of the permission levels accords the SharePoint objects you select for this plan.

  ***Note**: Selecting this option will slow down the search speed.

8. When finished, click **Next** on the ribbon. The **Search Filter** screen appears.

9. Specify the SharePoint object levels where you want to search for specific permissions by selecting the corresponding checkboxes. Only the permissions for the selected levels will be included in the search result. Limiting the search scope by **Search Level** will greatly improve Security Search Performance and provide more accurate results.

7. Use the drop-downs to add a filter rule specifying which objects or data within each SharePoint level will be searched. Click **Add** to add the rule to the list. For more information related to search filters, refer to [Appendix A: Search Filter Table](#).

- Change the logical relationship between two or more filter rules by clicking **And** or **Or** to the right of the list entry.

  - o **And** – The content that meets all the rules is displayed.

  - o **Or** – The content that meets one of the rules is displayed.

- The **Basic Filter Conditions** field lists the logical relationship between the filter rules.

- If desired, click the down arrow beside the filter rule number to reorder filter rules of the same level.

  ***Note**: If no filter policy is specified in the **Search Filter** pane, all objects or data under the specified nodes are searched.

10. When you're finished setting up filter rules, click **Next** on the ribbon. The **Schedule Selection** screen appears.

11. Select a scheduling option:

- **No Schedule** – Select this option to run a security search without a schedule.

- **Configure the Schedule Myself** – Select this option to configure a customized schedule, and run the security search by schedule. Fill in the parameters according to your desired schedule. After configuring the schedule for the search, click **Calendar View** to view the scheduled search by day, week, or month.

12. When finished, click **Next** on the ribbon. The **Notification** screen appears.

13. Select a previously-created user notification profile from the **Notification** drop-down list, or select **New Notification** to configure a new user notification. Refer to the User Notification Settings section in the [DocAve 6 Control Panel Reference Guide](#) for instructions on configuring user notification.

    *Note: Click **View** to the drop-down list to view the detailed information of the selected user notification profile.

14. When finished setting up notifications, click **Next** on the ribbon. The **Overview** screen appears.

15. Review and edit the plan selections. To make changes, click **Edit** to the right of the row. This links to the corresponding setting page, allowing you to edit the configuration.

16. Click **Finish** or **Finish and Run Now** on the lower-right section of the screen. The security search plan is now listed in Plan Manager.

Refer to [Appendix C: Security Search Result](#) for a table of actions that can be performed after a security search.

Performing a Security Search using Security Search Form Mode

Security Search Form Mode offers the ability run a quick security search by providing a truncated version of all of the Search Wizard screens on one page. Click **Security** > **Security Search** > **Security Search Form Mode**. For detailed information about how to configure a security search condition, refer to [Performing a Security Search using Security Search Wizard](#).

*Note: If you are unfamiliar with this feature, it is not recommended that you use this search mode to run a security search.

Refer to [Appendix C: Security Search Result](#) for a table of actions that can be performed after a security search.

Using a Predefined Search

Start with a Predefined Search offers the ability to apply a predefined search profile on a newly-specified scope. To start a predefined search, complete the following steps:

1. Select the **Scope** of the content, as described in [Selecting Farms and Nodes](#).

2. Click **Management** or **Security** > **Admin** or **Security Search** > **Start with a Predefined Search**. The predefined search screen appears.

3. Select a predefined search profile from the drop-down list. The information for the selected search job displays in the **Summary** section.

4. Click **Search** from the lower-right section of the screen to start this search job.

*__Note__: Ensure that the predefined search profile is applied on a scope level no lower than the top filter level specified in the search profile. For example, if you have set up search filter rules on the site collection level and site level in a predefined profile, the node level for starting with a predefined search must be equal to or higher than site collection level.

Managing Content

Refer to the topics below for information related to SharePoint content management. Content management in Administrator focuses on the centralization of content-related operations (existing ones in SharePoint and new functions implement in DocAve).

Creating Site Collections and Content Databases

To create a site collection or content database in DocAve Administrator, complete the following steps:

1. Select the Web application to create a new site collection/content database in, as described in Selecting Farms and Nodes.

2. Click the **Management** tab.

3. Click **New** > **New Site Collection** or **New Content Database**. The applicable configuration screen appears.

This functionality also exists within SharePoint 2010 and SharePoint 2013. For more information on creating content databases, Web applications, site collections, sites, lists/libraries, folders, files, and items, refer to SharePoint Help. To view tables presenting operations that are shared between DocAve and SharePoint at various levels, refer to Appendix B: DocAve Administrator and SharePoint Operations.

Deploying Site Maximum Depth

Use the Deploy Site Maximum Depth feature to set up the maximum number of subsites that can be created in a site collection. Limiting the number of subsites can help reduce the amount of content sprawl within a database.

To deploy a site maximum depth, complete the following steps:

1. Select the farm or node to add content to, as described in Selecting Farms and Nodes.

2. By default, the **No Limit** option is selected. To create sites without the limit of maximum depth. Click **Configuration** > **Deploy Site Maximum Depth**.

3. Select the **Maximum Depth** radio button.

4. Define the maximum depth of the selected site collection by inputting a positive number into the field.

   For example, assume the number inputted is 2. If **SiteCollection1** has a sub-site named **Site1**, and then you attempt to create a site under **Site1**, an error occurs with a prompt.

   *Note: The number entered cannot be less than the current site depth.

5. Click **OK** to apply the setting.

Extending Web Applications

Extend an existing Web application if you need to have separate IIS Web sites that expose the same content to users. This option is typically used for extranet deployments where different users access content using different domains. It reuses the same content databases from the selected Web application.

To extend a Web application, complete the following steps:

1. Select the Web application to extend, as described in Selecting Farms and Nodes.

2. Click the **Management** tab.

3. Click **Extend**. The Extend configuration screen appears.

This functionality also exists within SharePoint 2010 and SharePoint 2013. For more information on extending Web applications, refer to SharePoint Help. To view tables presenting operations that are shared between DocAve and SharePoint at various levels, refer to Appendix B: DocAve Administrator and SharePoint Operations.

*Note: The site collection can be created in the specified content database through DocAve, but it cannot be directly created in the specified content database in SharePoint.

Moving Site Collections across Content Databases

Use the **Change Content Database** feature to move a selected site collection from its own content database to another content database. At least two content databases are required to use this functionality. This is useful in ensuring you conform to Microsoft's recommended guidelines for content database sizes, and provides alternatives for restructuring environments that have been deployed with poor information architecture or sizing guidelines.

To move a site collection to another content database, complete the following steps:

1. Select a node on the site collection level, as described in Selecting Farms and Nodes.

2. Click **Management** > **Move**. The **Move** configuration screen appears.

3. Configure the following options:

   - **Move to Another Database** – Select the destination content database. In this field, view the selected Site Collection URL and the detailed information of available content databases.

   - **Advanced Settings** – If desired, select **Allow Shallow Copy** and specify a provider name. If you select this option, the stubs in the source site collection remain stubs after moving the source site collection to another content database. If you do not select this option, the stubs in the source site collection become real data after moving the source site

collection to another content database. This means that the data is stored in SQL instead of stored in the external storage.

- **Schedule Selection** – Choose whether or not to use a schedule. If configuring the schedule yourself, input a start time. This operation does not take the sites offline. When performing this operation, DocAve locks the sites as **Read-only**.

- **Notification** Select a previously-created user notification profile from the **Notification** drop-down list, or select **New Notification** to configure a new user notification. Refer to the User Notification Settings section in the DocAve 6 Control Panel Reference Guide for instructions on configuring user notification.

  ***Note**: Click **View** to the drop-down list to view the detailed information of the selected user notification profile.

4. Click **OK** to start the job. Access Job Monitor to view job details.

Checking for Broken Links

The **Check Broken Link** feature searches for the broken links that cannot be accessed in SharePoint. We recommend running this rule following restructuring, replication, or any other type of content migration to ensure the integrity of data. This can also be run proactively as a "good housekeeping" job to ensure SharePoint users have the best experience in navigation. It then generates a job report, which includes information such as searched pages, searched URLs, and broken links.

To check broken links, complete the following steps:

1. Select the scope of the content (i.e. site collection level and site level), as described in Selecting Farms and Nodes.

2. Click **Management** > **Check Broken Link**. The **Check Broken Link** screen appears.

3. Enter a **Plan Name** for the plan. A plan name with the format **Check Broken Link HH:MM:SS YYYY-MM-DD** is provided by default.

    - Click **Check** to the plan name to check whether the specified plan name is available. A green check mark indicates that the specified plan name is available. A warning message appears if the specified plan name already exists and some suggested plan names are listed beneath.

    - Add an optional **Description** if desired.

4. Select the desired **Link Type Selection** to search.

    ***Note**: Links in documents and files cannot be checked.

5. Specify the number of times that DocAve Administrator will attempt to verify that a link is broken in the **Retry Count Limit** field. If DocAve Administrator fails to access the link after retrying the specified number of times, the link is regarded as broken.

- **Internal links depth limit** – Input a positive number to limit the internal links depth. Internal links point to SharePoint content.

- **External links depth limit** – Input a positive number to limit the external links depth. External links point to non-SharePoint content.

For example, assume linkA is on page1. LinkA points to page2, which contains linkB1, linkB2, linkB3. LinkB1 points to page3, which has linkC1, linkC2, linkC3. LinkC1 points to page4, which contains linkD1 and linkD2. LinkA, linkB1, linkC2, and linkD2 are internal links. LinkB2, linkC1, linkC3, and linkD1 are external links.

If Internal links depth limit is 2, and External links depth limit is 4, linkA, linkB1, linkB2, linkB3, linkC1, linkC3 and linkD1 are checked, while linkC2 and linkD2 are not checked.

6. Select the **URL Filter** policy for the URL scan.

- **No Filter** – Select it to check all the links' URLs.

- **Include URLs that match the criteria** – Select it and specify the URL of the links that you want to check. In the displayed area, enter the full URL or keywords of the links to specify the checking scope before performing the broken links checking job. If entering a keyword, all URLs that contain the keyword will be associated.

- **Exclude URLs that match the criteria** – Select it and specify the URL of the links that you do not want to check. In the displayed area, enter the full URL or keyword of the links to specify the checking scope before performing the broken links checking job. If entering a keyword, all URLs that contain the keyword will be associated.

7. Select a scheduling option.

- **No Schedule** – Select this option to run an admin search without a schedule.

- **Configure the Schedule Myself** – Select this option to configure a customized schedule, and run the admin search by schedule. Fill in the parameters according to your desired schedule. After configuring the schedule for the search, click **Calendar View** to view the scheduled search by day, week, or month.

8. When finished configuring the schedule, click **Next**. The **Notification** screen appears.

9. Select a previously-created user notification profile from the **Notification** drop-down list or select **New Notification** to configure a new user notification. Refer to the User Notification Settings section in the DocAve 6 Control Panel Reference Guide for instructions on configuring user notification.

You can click **View** to the drop-down list to view the detailed information of the selected user notification profile.

10. Click **Save and Run Now** or **Save** on the lower-right section of the screen. The broken link search plan is now listed in Plan Manager.

Searching Web Parts

The **Search Web Parts** feature allows you to search a specified Web part and perform further operations on the search results.

Search Web Parts

To search Web parts, complete the following steps:

1. Click **Management** tab > **Search Web Parts**. The Search Web Parts page appears.

2. Enter a **Plan Name**. A plan name with the format **Search Web Part HH:MM:SS YYYY-MM-DD** is provided by default.

   - Click **Check** next to the plan name to check whether the specified plan name is available. A green check mark indicates that the specified plan name is available. A warning message appears if the specified plan name already exists and some suggested plan names are listed beneath.

   - Add an optional **Description**.

3. Add a **Search Filter** rule to select specific objects or data within Web application level, site collection level, and site level.

Rule	Condition	Value	Result
Title	Contains	len	The Web part whose title contains **len** is displayed.
	Equals	Announcements	The Web part whose title is **Announcements** is displayed.
Template Name	Contains	DataAssociation	The Web part whose template name contains **DataAssociation** is displayed.
	Equals	AuthoredListFilter. webpart	The Web part whose template name is **AuthoredListFilter** is displayed.
Page URL	Contains	AnalyticsReports	The Web part whose page URL contains **AnalyticsReports** is displayed.
	Equals	http://test:2000/R eports List/AllItems.aspx	The Web part whose page URL is **http://test:2000/Reports List/AllItems.aspx** is displayed.

4. Schedule Selection – Choose whether or not to use a schedule.

   - **No Schedule** – Run the plan without a schedule.

   - **Configure the Schedule Myself** – Select this option to configure a customized schedule, and run the Web parts search by schedule. Fill in the parameters according to your desired schedule. After configuring the schedule for the search, click **Calendar View** to view the scheduled search by day, week, or month.

5. Select a previously-created user notification profile from the **Notification** drop-down list or select **New Notification** to configure a new user notification. Refer to the User Notification

Settings section in [DocAve 6 Control Panel Reference Guide](#) for instructions on configuring user notification.

You can click **View** to the drop-down list to view the detailed information of the selected user notification profile.

6. Click **OK** or **OK and Run Now**. The plan is now available in Plan Manager.

Further Operations for Search Web Parts in Job Monitor

If the job completes successfully, access Job Monitor for further operations by completing the following steps:

1. Select the Web part job you wish to work with. **Web Part Management** appears in the ribbon.

2. Click Web Part Management.

3. Select the Web part that you want to perform further options on; the following operations will be enabled.

    - **Remove Web Part** – Delete the selected Web part.

    - **Reset Web Part** – Reset the selected Web part.

    - **Close Web Part** – Close the selected Web part.

Changing Item Metadata

The Change Metadata feature allows you to change the metadata of the items in a list/library. Meanwhile, you can change the specified item's metadata by using the online or offline method.

Changing Item Metadata Online

When using the online method to change the item's metadata, the changed metadata in DocAve will be synchronized to the corresponding item in SharePoint.

To change the metadata of items included in a list/library online, complete the following steps:

1. Select the **Scope** of the content, as described in [Selecting Farms and Nodes](#). Only the item level is supported for the **Change Metadata** feature.

2. Click **Management** > **Change Metadata** > **Online**. The **Change Metadata (Online)** screen appears.

3. In the **Update Column Value** field, select an existing SharePoint column from the drop-down list and click **Add** to add this column for changing its value.

4. When the column is added, enter the new value in the **New Value** text box to replace the original value of the specified column.

5. Click **OK** to complete changing the column metadata and synchronize the change to the corresponding item in the SharePoint list/library.

Changing Item Metadata Offline

When using the offline method to change the item's metadata, you can export the metadata information of the selected items as a file to the specified file system location. After completing the modification of the metadata in the exported file, you can import the modified file back into DocAve.

To change the metadata of the items included in a list/library offline, complete the following steps:

1. Select the **Scope** of the content, as described in [Selecting Farms and Nodes](#).

   *Note: Only the item level is supported for the Change Metadata feature.

2. Click **Management** > **Change Metadata** > **Export Configuration File**. The Change Metadata (Export Configuration File) screen appears.

   - **Select Columns** – Select the existing SharePoint columns from the drop-down list to export the metadata.

   - **Download Settings** – Select a downloading location type for storing the report.

     o **Export to local immediately** – Select this option to download the report to the local file system location of the currently used server.

     o **Offline export** – Select this option to download the report to the location on the specified server. When selecting this option, the following settings are displayed as the further configuration.

       ▪ **Export Location** – Select an existing export location from the drop-down box to store the report before downloading.

       ▪ **Notification** –To notify the specified users of the status about this export job, select a previously-created notification profile form the drop-down list, or click **Create a New Profile** to create a new one. For more information about creating a new notification profile, refer to the [DocAve 6 Control Panel Reference Guide](#). You can also click **View** next to the textbox to view the detailed information of the selected notification profile.

3. After the configuration settings above, click **OK** to start the download operation. After completing downloading, the Metadata Configuration Report will be stored to the specified location as a **Metadata_Configuration_Report_Serial Number.zip** file.

   *Note: By default, the maximum number of items whose metadata can be exported at one time is 5000. This limitation is set to ensure DocAve can run smoothly. To change the limitation, navigate to the path *…\AvePoint\DocAve6\Manager\Control\Config\CentralAdmin\CentralAdminWebUtility.config* to change the value of **CASearchQuotas**.

4. Extract the **Metadata_Configuration_Report_Serial_Number.zip** file.

5. In the **Metadata_Configuration_Report_Serial_Number** folder, open the **Metadata_Configuration_File_Serial_Number.xls** file.

6. Prior to changing the metadata of a particular item, set the value of the **Allow Change** column to **Yes** in the corresponding row.

7. Change the metadata of the items by editing the values in the corresponding columns.

8. Save the modifications and close the file.

9. After the configuration of the corresponding XLS file is done, navigate to **DocAve 6** > **Administration** > **Administrator**, select the item level nodes where you want to import the Configuration File on the tree and click **Management** > **Change Metadata** > **Import Configuration File**. The Change Metadata (Import Configuration File) screen appears.

   - **Import Configuration File** – Click **Browse** and select the configured exported file from the file system location.

   - **Schedule** – Select the schedule type for this profile to use.

     o **No Schedule** – Select this option to run the import job immediately.

     o **Start Time** – Specify the time when the import job starts.

   - **Notification** - To notify the specified users of the status about this import job, select a previously-created notification profile form the drop-down list, or click **New Notification** to create a new one. For more information about creating a new notification profile, refer to DocAve 6 Control Panel Reference Guide. You can also click **View** next to the textbox to view the detailed information of the selected notification profile.

10. Click **OK** to save the configuration and start to run the import job.

Searching Alerts

Search Alert allows you to search the alerts for specified list/library or search alerts of certain users for specified list/library. In order to build a plan, select the site level, and then click **Security** > **Alert Me** > **Search Alerts.**

To use Search Alerts, complete the following steps:

1. Select the users whose alerts you want to search.

   - **All users** – Select **All users** to search for the alerts set for all users within the selected scope.

   - **Display alerts for** – Select **Display alerts for** and enter the users whose alerts you wish to search. Click the **Check Names** ( ) button to verify the inputted names, or click the **Browse** ( ) button to browse through the names.

2. Select the lists/libraries in the **Scope** section where you want to search the alerts.

3. Select the **Frequency** by which you want to perform a search.

4. Specify the **Alert Title** that you want to search.

5. Click **OK** to start the search.

6. After running the job, the search results are listed in the **Search Result** list. The following operations are available:

- **New** – Create an alert.

- **Edit** – Edit the selected alert.

- **Delete** – Delete the selected alert.

- **Enable** – Enable the application of selected alert on relevant list/library.

- **Disable** – Disable the application of selected alert on relevant list/library.

Deleting Web Applications

DocAve Administrator offers the ability to delete an entire SharePoint Web application and, optionally, all of its contents and settings. To delete a Web application, complete the following steps:

1. Select the Web application level to be deleted, as described in Selecting Farms and Nodes.

2. Click the **Management** tab.

3. Click **Delete** > **Delete Web Application**. The Delete Web Application screen appears.

This functionality also exists within SharePoint 2010 and SharePoint 2013. For more information on deleting Web applications, refer to SharePoint Help. To view tables presenting operations that are shared between DocAve and SharePoint at various levels, refer to Appendix B: DocAve Administrator and SharePoint Operations.

Deleting Orphan Sites

A site becomes an orphan site when the URL path of the site collection where it resides is inaccessible. A site collection might become inaccessible while you're trying to attach a content database to a Web application. If a site collection in the Web application uses the same site collection URL as a site collection in the content database you are attaching, the site collection being attached will be inaccessible. All of the sites within this site collection become orphan sites.

To delete the orphan sites, use the **Delete Orphan Sites** feature. There are two modes that can be used for deleting an orphan site: **Run the Orphan Site Scan as a job and save the plan for later use** and **Scan for Orphan Site now**. The **Scan for Orphan Site now** mode performs a scan in which the user waits for a system response or report before any further actions can be performed. The **Run the Orphan Site Scan as a job and save the plan for later use** mode initiates a scan in the background of DocAve, enabling the user to continue navigating through the user interface without worrying about prematurely ending the action, and the scan will be saved as a plan for later use.

To remove orphan sites, complete the following steps:

1. Select a node on the Web application level, as described in [Selecting Farms and Nodes](#).

2. Click **Management** > **Delete Orphan Sites**. The **Delete Orphan Sites** screen appears.

3. Select **Run the Orphan Site Scan as a job and save the plan for later use** or **Scan for Orphan Site now**. Proceed to the section below that is appropriate to your selection.

Running the Orphan Site Scan as a Job and Saving the Plan for Later Use

The **Run the Orphan Site Scan as a job and save the plan for later use** option initiates a back-end scan which generally takes longer to complete than front-end scans; however, you can continue to navigate through the DocAve user interface while a back-end scan is running. To run the Orphan Site Scan as a job and save the plan for later use, complete the following steps:

1. Enter a **Plan Name** for the plan. A plan name with the format **Delete Orphan Site HH:MM:SS YYYY-MM-DD** is provided by default.

   - Click **Check** to the plan name to check whether the specified plan name is available. A green check mark indicates that the specified plan name is available. A warning message appears if the specified plan name already exists and some suggested plan names are listed beneath.

   - Add an optional **Description** if desired.

2. For the **Verify Sites before Deleting** section, choose whether or not to verify the sites in Job Monitor before deleting them. For security reasons, it is recommended that you verify sites before deletion. For more information about verifying the sites in Job Monitor, refer to Additional Operations for Deleting Orphan Sites in [Job Monitor](#).

   - **Yes** enables you to view the orphan sites searched by DocAve in Job Monitor instead of deleting them directly.

   - **No** removes the orphan sites directly.

3. Click **Next** on the ribbon. The Schedule and Notification screen appears.

4. Select a scheduling option.

   - **No Schedule** – Select this option to delete orphan sites immediately.

   - **Configure the Schedule Myself** – Select this option to configure a customized schedule, and run the search by schedule. Fill in the parameters according to your desired schedule. After configuring the schedule for the search, click **Calendar View** to view the scheduled search by day, week, or month.

5. Select a previously created user notification profile from the **Notification** drop-down list. Or select **New Notification** to configure a new user notification. Refer to the User Notification Settings section in the [DocAve 6 Control Panel Reference Guide](#) for instructions on configuring user notification.

You can click **View** to the drop-down list to view the detailed information of the selected user notification profile.

6. When finished setting up notifications, click **Next** on the ribbon. The **Overview** screen appears.

7. Review and edit the plan selections. To make changes, click **Edit** to the right of the row. This links to the corresponding setting page, allowing you to edit the configuration.

8. Click **Finish** or **Finish and Run Now** on the lower-right section of the screen. The Delete Orphan Site plan is now listed in Plan Manager.

Scanning For Orphan Sites Now

The **Scan for Orphan Site now** option initiates a front-end scan which can be completed faster than a back-end scan; however, navigating away from the current user interface screen will terminate the scan. If you want to scan now on the front-end, complete the following steps:

1. After selecting **Scan for Orphan Site now**, the following message appears: **Scan a specific scope for orphan sites. It may take some time. Click here to start.** Click **here** to begin the orphan site scan.

2. When the scan completes, the orphan sites within the specified scope are listed under the **Site Collection URL** field.

3. Select the orphan sites to remove.

   - To add or remove columns, click ⊕ on the upper-left of the table. Select or deselect the columns as desired. Click **OK** to apply your selections.

   - Hide columns by placing the cursor over the relevant column name and clicking ⊖.

   - To quick-search an orphan site, input the keywords into the **Input Keyword** field and click **Search** icon to start the search.

   - Initiate a search based on the content of a specific column by placing the cursor over relevant column name, clicking ▽ icon, and inputting the content to search by.

   - **Search all pages** searches for an orphan site across all pages, while **Search current page** searches for the orphan site in the current page.

4. Select a scheduling option.

   - **No Schedule** – Select this option to run the job without a schedule.

   - **Configure the Schedule Myself** – Select this option to configure a customized schedule, and run the job by schedule. Fill in the parameters according to your desired schedule. After configuring the schedule for the search, click **Calendar View** to view the scheduled search by day, week, or month.

5. Select a previously created user notification profile from the **Notification** drop-down list. Or select **New Notification** to configure a new user notification. Refer to the User Notification Settings section in the <u>DocAve 6 Control Panel Reference Guide</u> for instructions on configuring user notification.

You can click **View** to the drop-down list to view the detailed information of the selected user notification profile.

6. When finished setting up notifications, click **Next** on the ribbon. The **Overview** screen appears.

7. Review and edit the plan selections. To make changes, click **Edit** to the right of the row. This links to the corresponding setting page, allowing you to edit the configuration.

8. Click **Finish** or **Finish and Run Now** on the lower-right section of the screen. The Delete Orphan Site plan is now listed in Plan Manager.

Additional Operations for Deleting Orphan Sites in Job Monitor

If you select **Yes** for the **Verify Sites before Deleting** option, further delete orphan site operations are available in Job Monitor. To configure additional operations for deleting orphan sites in Job Monitor, complete the following steps:

1. In Job Monitor, select the job/plan you want to run. Click **Orphan Sites Deletion** after it appears on the ribbon.

2. On the **Orphan Sites Deletion** page, view and select the orphan sites that you want to delete.

3. Click **Next** to configure the schedule and notification. For details on these configurations, refer to Scanning .

4. When finished setting up notifications, click **Next** on the ribbon. The **Overview** screen appears.

5. Review and edit the plan selections. To make changes, click **Edit** to the right of the row. This links to the corresponding setting page, allowing you to edit the configuration.

6. Click **Finish** or **Finish and Run Now** on the lower-right section of the screen. The Delete Orphan Sites plan is now listed in Plan Manager.

Searching for Duplicate Files

The **Search Duplicate Files** feature allows you to search for the files with the same name and extension name from the specified scope. The feature is supported for Farm, Web Application, Site Collection and Site levels. To set up a search duplicate files plan, complete the following steps:

1. Click **Management** tab > **Search Duplicate Files**. The Search Duplicate Files page appears.

2. Enter a **Plan Name**. A plan name with the format **Search Duplicate File HH:MM:SS YYYY-MM-DD** is provided by default.

    -   Click **Check** to the plan name to check whether the specified plan name is available. A green check mark indicates that the specified plan name is available. A warning message appears if the specified plan name already exists and some suggested plan names are listed beneath.

    -   Add an optional **Description**.

3. Configure **Search Criteria** according to your requirements:

    - **Files in document libraries** – Specify whether to search for files from the document libraries in the specified scope.

    - **Attachments to list items** – Specify whether to search for files from the attachments of the lists in the specified scope.

    - **Include file extensions only** – Specify the file types you want to search for from the drop-down list. The file extensions displayed in the drop-down list can be modified in a DocAve configuration file. Refer to Configuring CentralAdminDuplicateFilesCommonFileNames2010.xml for more information.

    - **Exclude files** – Specify the files that you do not want to search for from the drop-down list. The files displayed in the drop-down list can be modified in a DocAve configuration file. Refer to Configuring CentralAdminDuplicateFilesCommonFileNames2010.xml for more information.

    - **Minimum number of duplicates** – Specify a number and only when the number of duplicate files reach or exceed the specified number, the duplicate files are searched.

    - **File size matching** – Only the duplicate files with the same size are searched if this option is enabled.

        *Note: The size matching's accuracy is 1 KB. Size values outside of the accuracy scope are not displayed.

    - **File name contains** – Enter a keyword and only the duplicate files whose name contain this keyword are searched.

4. **Schedule Selection** – Choose whether or not to use a schedule.

    - **No Schedule** – Run the plan without a schedule.

    - **Configure the Schedule Myself** – Select this option to configure a customized schedule, and run the duplicate files search by schedule. Fill in the parameters according to your desired schedule. After configuring the schedule for the search, click **Calendar View** to view the scheduled search by day, week, or month.

5. Configure user **Notification** settings. Select a previously created notification profile from the drop-down list, or select to create a New Notification. Refer to the User Notification Settings section in the DocAve 6 Control Panel Reference Guide for more information about creating a new notification.

    You can click **View** to the drop-down list to view the detailed information of the selected user notification profile.

6. Click **OK** and the plan is now available in **Plan Manager**. Or click **OK and Run Now** to run the search job immediately. Access **Job Monitor** to view job details and download the job report.

Right-Click Operations on Each Level

When selecting the node from the **Scope** panel in Administrator, right-click on the node for quick access to chief functions. The following table displays the chief functions supported on each level.

Level	Option Name	Ribbon Feature
Farm	Refresh	N/A
Web Application	Refresh	N/A
	General Settings	General Settings
	Permission Policy	Permission Policy
	Dead Account Cleaner	Dead Account Cleaner
Site Collection	Refresh	N/A
	Copy URL	N/A
	Open in Browser	N/A
	New Site	New
	Dead Account Cleaner	Dead Account Cleaner
	Check Broken Link	Check Broken Link
	Move Site Collection	Move
	Permission Levels	Permission Levels
Site	Refresh	N/A
	Copy URL	N/A
	Open in Browser	N/A
	Dead Account Cleaner	Dead Account Cleaner
	Check Broken Link	Check Broken Link
	Clone Site Permissions	Clone Site Permissions
	New Site	New Subsite
List/Library	Refresh	N/A
	Copy URL	N/A
	Open in Browser	N/A
	List Permissions	List Permissions
	Alert Me	Set alert on this list/library
	Delete	Delete
	Versioning Settings	Versioning Settings
Folder	Refresh	N/A
	Copy URL	N/A
	Open in Browser	N/A
	New	New
	Delete	Delete
Item	Refresh	N/A
	Delete	Delete

Managing Security

Refer to the topics below for information related to security management in DocAve Administrator.

Granting User Temporary Permissions

The Grant User Temporary Permissions feature allows you to grant the permissions for the users or groups in SharePoint. The granted permissions will be implemented on the selected nodes for a certain period of time. Once the period expires, these users or groups' granted permissions will be deleted and not be implemented any more.

To grant the user temporary permissions, complete the following steps:

1. Select the **Scope** of the content (from site collection level to list/library level), as described in [Selecting Farms and Nodes](#).

   *Note: If you want to grant the temporary permission to the specified users or groups, you must make sure the selected nodes on the farm tree have broken inheritance from the parent nodes.

2. Click **Security** > **Grant Permissions** > **Grant Temporary Permissions**. The Grant Temporary Permissions screen appears.

3. Enter usernames, group names, or the users' e-mail addresses in the **Select Users** field. The username entered in the text box is supported for Active Directory users, Form Based Authentication users, and SharePoint users. The group name entered in the text box is supported for Active Directory group and Form Based Authentication role. Click the **Check Names** icon to verify the name you entered, or click the **Browse** icon to browse through a list of names.

4. Select one or multiple permission levels in the **Grant Permissions** field to grant the specified users or group permissions.

5. Specify a duration time for the implemented granted permissions in the **Expiration Time** field.

6. Select the **Send welcome e-mail to the new users** checkbox in the **Send E-Mail** field to send an e-mail to the users when the temporary permissions are granted to them.

7. Click **OK** to complete granting permissions to the specified users and groups.

Once the temporary permissions are granted to the specified users and groups on the selected nodes, a temporary SharePoint group will be created in the corresponding SharePoint site by DocAve. The temporary SharePoint group includes the users and groups that are granted the temporary permissions. When the temporary permissions expire, the temporary SharePoint group will be deleted automatically from SharePoint.

*Note: The temporary SharePoint groups with the same expiration time can be distinguished by the group name's suffixes (underscore and the number of the order they are created, such as DocAve_Temporary Group_20130629160000_1 and DocAve_Temporary Group_20130629160000_2).

Searching User Temporary Permissions

The Search Temporary Permissions feature allows you to search and manage the temporary permissions for users and groups within the selected scopes. To search the temporary permissions, complete the following steps:

1. Select the **Scope** of the content (from farm level to list/library level), as described in Selecting Farms and Nodes.

2. Click **Security** > **Grant Permissions** > **Search Temporary Permissions**. The **Search Temporary Permissions** screen appears.

3. In the **Search Temporary Permissions** pane, select one or multiple object levels (site collection, site, and list) in the **Search Level** area to include the users or groups that are granted the temporary permissions and click **Search**. Or, enter the keywords included in a URL, and then click **Search**.

4. When the search completes, the search results will be displayed in the **Search Result** area. Select the corresponding checkboxes of the search results and click **Edit Temporary Permissions** to edit the users or groups temporary permissions or click **Delete Temporary Permissions** to delete the users or groups temporary permissions permanently.

Cloning User Permissions

The Clone User Permissions feature allows you to copy a user's or group's permissions to one or more specified users/groups. To clone the user permissions, complete the following steps:

1. Select the **Scope** of the content (from farm level to folder level), as described in Selecting Farms and Nodes.

2. Click **Security** > **Clone Permissions** > **Clone User Permissions**. The **Clone User Permissions** screen appears.

3. Enter a username or group name in the **Clone User Permissions from** field. This user/group is the source account of permissions to be cloned. Note that the user/group you enter must exist under the selected scope. Click the **Check Names** icon to verify the inputted name, or click the **Browse** icon to browse through a list of names.

4. Enter a username or group name in the **Clone User Permissions to** field. This user/group is the destination account of permissions to be cloned.

5. Select a previously created filter policy from the **Filter Policy** drop-down list. A filter policy allows you to clone the user permissions with certain conditions. Refer to the Configuring Filter Policies section in the DocAve 6 Control Panel Reference Guide for more information on creating a new filter policy.

6. Select a Permission Option. This determines how you will assign the source user's/group's permission to the destination user/group.

    - **Append** – Adds the permission of the source user/group to the destination users/groups.

    - **Replace** – Replaces the destination permission with the source permission.

7. Select an **Additional Option** for the source user if it is a member of a group.

    - **Add target users to the source user's group** – Adds the destination user to the group where source user exists.

      For example, assume that user1 is a dead account that exists in SharePoint group1, and user2 is user1's destination user. If **Add target users to the source user's group** is selected, user2 is added into group1.

    - **Clone source user's group permission to target users directly** – Copies the permissions of the group where the source user exists to the destination users.

8. Manage source user and group in **Options for Transfer**.

    - **Remove source user's explicit permissions or group's permissions** – Removes the source user's or group's permission after cloning the permission successfully.

    - **Remove source user from SharePoint groups** – Deletes the source user from SharePoint Groups after cloning the permission successfully.

    - **Delete source user or group from site collection** – Deletes source user or group from site collection after cloning permission successfully.

9. Select whether or not to turn on **User Alert Properties**. If **Yes** is selected, this copies the user alerts settings set by the source user to the destination users. Note that this is not supported for Office 365 sites.

10. Choose whether or not to **Change Metadata**. If **Yes** is selected, this transfers the corresponding source user's metadata to destination users. Enter the metadata column name and click **Add** to add it. Note that this is not supported for Office 365 sites.

11. Choose whether or not to **Include Detailed Report** of this clone job in Job Monitor.

12. Select a scheduling option.

    - **No Schedule** – Select this option to run an admin search immediately.

    - **Configure the Schedule Myself** – Select this option to configure a customized schedule, and run the job by schedule. Fill in the parameters according to your desired schedule. After configuring the schedule for the search, click **Calendar View** to view the scheduled search by day, week, or month.

13. Select a previously created user notification profile from the **Notification** drop-down list. Or select **New Notification** to configure a new user notification. Refer to the User Notification Settings section in the [DocAve 6 Control Panel Reference Guide](#) for instructions on configuring user notification.

You can click **View** to the drop-down list to view the detailed information of the selected user notification profile.

14. When satisfied with your selections, click **OK** to start the job. Access Job Monitor to view job details and download the job report.

Cloning Site Permissions

The Clone Site Permissions feature allows you to copy source users/groups and permissions to one or more destination sites. Both SharePoint default permissions and user-defined permissions can be cloned. To clone the site permissions, complete the following steps:

1. Select the **Scope** of the content (from farm level to folder level), as described in Selecting Farms and Nodes.

2. Click **Security** > **Clone Permissions** > **Clone Site Permissions**.

3. **Select the user account(s)** you wish to clone to the destination sites by selecting the corresponding checkbox. Click the **Check Permission** link to view the permissions of the selected users or groups.

4. Expand the **Farm** tree to select the **Destination Sites** where you wish to clone permissions.

5. Choose a Conflict Option, which determines how to handle the permission conflict when the site permission in the source node does not match that of the destination node.

   - **Append** – Adds the permission of source user to destination permission.

   - **Replace** – Replaces destination permission with source permission.

   - **Skip** – Keeps destination permission as-is.

6. Select a scheduling option.

   - **No Schedule** – Select this option to run an admin search immediately.

   - **Configure the Schedule Myself** – Select this option to configure a customized schedule, and run the job by schedule. Fill in the parameters according to your desired schedule. After configuring the schedule for the search, click **Calendar View** to view the scheduled search by day, week, or month.

7. Select a previously created user notification profile from the **Notification** drop-down list. Or select **New Notification** to configure a new user notification. Refer to the User Notification Settings section in the DocAve 6 Control Panel Reference Guide for instructions on configuring user notification.

   You can click **View** to the drop-down list to view the detailed information of the selected user notification profile.

8. When satisfied with your selections, click **OK** to start the job. Access Job Monitor to view the job details and download the job report.

Using Dead Account Cleaner

Dead Account Cleaner allows you to remove deactivated and non-existent AD accounts from your SharePoint environment and transfer their permissions to other available users. See the topics below for more information.

*Note: The Dead Account Cleaner function does not support ADFS, so a deactivated or non-existent AD account's provider user who is ADFS-Certificated cannot be searched for or deleted through the use of Dead Account Cleaner in DocAve Administrator.

Using Plan Mode

To use the Plan Mode in Dead Account Cleaner, complete the following steps:

1. Select the **Scope** of the content (from farm level to site level), as described in Selecting Farms and Nodes.
2. Click **Security** > **Dead Account Cleaner**> **Plan Mode**.
3. Enter a **Plan Name** for the plan. A plan name with the format **Dead Account Cleaner HH:MM:SS YYYY-MM-DD** is provided by default.

   - Click **Check** to the plan name to check whether the specified plan name is available. A green check mark indicates that the specified plan name is available. A warning message appears if the specified plan name already exists and some suggested plan names are listed beneath.

   - Add an optional **Description** if desired.
4. Select a previously created filter policy from the **Filter Policy** drop-down list. A filter policy allows you to search for dead accounts using certain conditions. Refer to the Configuring Filter Policies section in the DocAve 6 Control Panel Reference Guide for more information on creating a new filter policy.
5. For the **Verify Accounts before Deleting** section, choose whether or not to verify the accounts in Job Monitor before deleting them. For security reasons, it is recommended that you verify accounts before deletion. For more information about verifying the accounts in Job Monitor, refer to Additional Operations for Dead Account Cleaner in Job Monitor.

   - **Yes** enables you to view the dead accounts searched by DocAve in Job Monitor instead of deleting them directly.

   - **No** removes the dead accounts directly. Selecting **No** enables the **Actions for My Site** and **Remove User Profiles from SSA** configuration options.
6. For the **Actions for My Site** section, choose whether to keep the My Sites of the dead accounts you are about to remove.

   - **Keep My Site** – Keeps My Sites of relevant dead accounts.

   - **Delete My Site** – Deletes My Sites of relevant dead accounts.

7. Choose whether or not to Remove User Profiles from SSA.

- **Keep User Profiles** – Keeps the user profiles.

- **Delete User Profiles** – Removes the user profiles of relevant dead accounts from SSA.

8. Select a scheduling option.

- **No Schedule** – Select this option to run an admin search immediately.

- **Configure the Schedule Myself** – Select this option to configure a customized schedule, and run the job by schedule. Fill in the parameters according to your desired schedule. After configuring the schedule for the search, click **Calendar View** to view the scheduled search by day, week, or month.

9. Select a previously created user notification profile from the **Notification** drop-down list. Or select **New Notification** to configure a new user notification. Refer to the User Notification Settings section in the <u>DocAve 6 Control Panel Reference Guide</u> for instructions on configuring user notification.

   You can click **View** to the drop-down list to view the detailed information of the selected user notification profile.

10. When satisfied with your selections, click **OK and Run Now** or **OK**. The plan is now listed in Plan Manager.

Using Scan Mode

Use Scan Mode to do a quick-search, which lists all of the dead accounts in your selected scope. You can perform further operations on the scan results.

To use Scan Mode, complete the following steps:

1. Select the **Scope** of the content (from farm level to site level), as described in <u>Selecting Farms and Nodes</u>.

2. Click **Security** > **Dead Account Cleaner** > **Scan Mode**.

3. After selecting Scan Mode, the following message appears: **Scan a specific scope for dead accounts. It may take some time. Click here to start.** Click **here** to begin the dead account scan.

4. When the scan completes, the dead accounts within the specified scope are listed under the **Username** field.

5. Select the dead accounts to remove.

- To add or remove columns, click the manage (⊕) buttons on the upper-left of the table. Select or deselect the columns as desired. Click **OK** to apply your selections.

- Hide columns by placing the cursor over the relevant column name and clicking the hide the column (⊖) button.

- To quick-search a dead account, input the keywords into the **Input Keyword** field and click **Search** icon to start the search.

- Initiate a search based on the content of a specific column by placing the cursor over relevant column name, clicking the filter the column (🔽) button, and inputting the content to search by.

- **Search all pages** searches for a user across all pages, while **Search current page** searches for the user in the current page.

6. Determine the dead account whose permission you want to transfer. Enter the destination username under the **Clone User Permissions** column. Click **Check Names** icon to verify the inputted usernames, or click **Browse** to browse through a list of names.

7. Click **Next** on the lower-right section of the page to access the **Options for Transfer Permissions** page.

8. Choose a Permission Option.

- **Append** – Adds the permission of source user to destination permission.

- **Replace** – Replaces destination permission with source permission.

9. Select whether or not to **Include Alerts**. If **Yes** is selected, this copies the user alerts settings set by the source user to the destination users.

10. Choose whether or not to **Change Metadata**. If **Yes** is selected, this transfers the corresponding source user's metadata to destination users. Enter the metadata column name and click **Add** to add it.

11. Select the **Permission Rule**. This determines how DocAve Administrator will handle the permissions of users in SharePoint groups.

- **Clone source user's group permission to target users directly**– Copies the permission of the group where the source user exists to destination user.

- **Add target users to the source user's group** – Adds the destination user to the group where source user exists.

  For example, assume that user1 is a dead account that exists in SharePoint group1, and user2 is user1's destination user. If **Clone source user's group permission to target users directly** is selected, group1's permission is cloned to user2.

12. For details on configuring the Options for Cleaning Dead Accounts options, refer to Using Plan Mode.

13. When satisfied with your selections, click **Finish**. The plan is now listed in Plan Manager.

Additional Operations for Dead Account Cleaner in Job Monitor

If you select **Yes** for the **Verify Accounts before Deleting** option, further delete Dead Account operations are available in Job Monitor. To configure additional operations for the Dead Account Cleaner in Job Monitor, complete the following steps:

1. In Job Monitor, select the job/plan you want to run. Click **Dead Account Cleaner** after it appears on the ribbon.

2. On the **Dead Account Deletion** page, view and select the dead accounts that you want to delete.

3. Click **Next** to configure the settings for transferring permissions and cleaning dead accounts.

   - For details on configuring Transfer Permissions options, refer to Using Plan Mode.

   - For details on configuring Cleaning Dead Accounts options, refer to Using Scan Mode.

4. Click **OK** to run the job.

Exporting, Editing, and Importing Configuration Files

In some cases, it might be desirable to export the permission (configuration) file for editing and to import the file later. This would be useful for those who find it easier to edit the permissions using Excel, versus using the DocAve Administrator user interface.

Exporting Configuration Files

Export the permission (configuration) file for editing by following the instructions in the procedure below.

Exporting SharePoint Groups and Users from a Security Search Result

To export a configuration file that contains SharePoint groups and users from a security search result for editing, complete the following steps:

1. Perform a security search, as described in Previewing Files in SharePoint Using the DocAve Preview Feature.

2. Access Job Monitor. When the search completes, select the job and click **Export for Editing** on the upper-right corner to pop up the **Export for Editing** window. Or you can also click **Search Result** to access to the **Search Result Tools** page and click **Export for Editing** to pop up the **Export for Editing** window.

3. In the **Export for Editing** window, select an export type for the selected job to download the report.

   - **Export to local immediately** – Select this option to download the report to the local file system location of the currently used server.

   - **Offline export** – Select this option to download the report to the location on the specified server. When selecting this option, the following settings are displayed as the further configuration.

     o **Export Location** – Select an existing export location from the drop-down box to store the report before downloading.

     o **Notification** – Select an existing notification profile from the drop-down box. A notification e-mail will deliver to the users who download the report.

After the configuration of the settings above, click **OK** to start the download operation.

Exporting SharePoint Groups on the Site Collection Level

To export SharePoint groups on the site collection level and the users in these groups for editing, complete the following steps:

1. Select the site collection you want to export groups, as described in [Selecting Farms and Nodes](#).

2. Click **Export Groups for Editing** on the ribbon under the **Security** tab. Save the file to a local drive.

Modifying an Exported Configuration File

Refer to the sections below to modify the configuration files exported from a security search result or Export Groups for Editing.

Modifying an Exported Configuration File from a Security Search Result

To modify an exported configuration file downloaded from a security search result, complete the following steps:

1. Navigate to the location on your local drive where the exported configuration file is saved. To export a configuration file, see [Exporting Configuration Files](#).

2. Unzip the report folder.

3. Open the configuration file to update the permissions.

4. Choose to **Add**, **Delete**, **Modify**, or **Inherit** the permissions. Update the status of the operation in the **Change** column accordingly.

   - **Add** – Adds a new permission to the specified target. If you want to add a new item to the configuration file, you must change the value of the **Change** column after adding the new information.

   - **Delete** – Deletes the permission for specific user by changing the value of the **Change** column to **Delete**.

   - **Modify** – Upon making a change on the specific item, the value of the **Change** column must be changed to **Modify**.

     *Note: Only the **User/Group** and **Permission** columns can be modified in the configuration file.

   - **Inherit** – Sets the selected node to inherit permissions from the parent node.

5. **Save** the configuration file after the update.

Modifying an Exported Configuration File Download by Export Groups for Editing

To modify an exported configuration file downloaded by Export Groups for Editing, complete the following steps:

1. Navigate to the location on your local drive where the exported configuration file is saved. To export a configuration file, see [Exporting Configuration Files](#).

2. Unzip the report folder.

3. Open the configuration file to update the group settings.

4. Choose to **Add** or **Delete** the groups or group members, and update the status of the operation in the **Action** column accordingly.

   - **Add** – To add a new group or add members into a group, add the information of the new group or group members in the corresponding row/cells, and change the value of the **Action** column to **Add**.

   - **Delete** – To delete a group or delete group members from a group, delete the information from the corresponding row/cells, and change the value of the **Action** column to **Delete**.

5. **Save** the configuration file after the update.

Importing a Configuration File

To import a configuration file back into SharePoint, complete the following steps:

1. After editing the configuration file (as described in Modifying an Exported Configuration File), you can import it to SharePoint by either of the following methods:

   - Access Job Monitor and randomly select a security search job. The **Search Result Tools** tab becomes enabled. Click **Import Configuration File.**

   - Select which farm you want to import the configuration file to and click **Import Configuration File** on the ribbon under the **Security** tab.

2. Select a configuration file type from the **File Type** drop-down box. **Edit User Permission** imports the file generated by security search, while **Edit Group** imports the file downloaded by **Export Groups for Editing**.

3. Select a farm from the **Farm Selection** drop-down box; the configuration file is applied to this farm. This option is not necessary if you choose to import the configuration file from **Security** > **Import Configuration File** at the farm level.

4. Click **Browse** to select which **Configuration File** to import.

5. In the **Options for Inherited Objects** area, choose whether to break the inherited objects' permissions inheritance from their parent nodes. This option is only supported for the **Edit User Permission** file type.

   - **Copy permissions from parent** – Keeps the nodes' permissions inheriting from the parent nodes.

   - **Clear permissions** – Remove all of the current permissions of the nodes that will stop inheriting permissions for the parent nodes.

6. Select a scheduling option.

   - **No Schedule** – Select this option to run an admin search immediately.

- **Configure the Schedule Myself** – Select this option to configure a customized schedule, and run the job by schedule. Fill in the parameters according to your desired schedule. After configuring the schedule for the search, click **Calendar View** to view the scheduled search by day, week, or month.

7. Select a previously created user notification profile from the **Notification** drop-down list. Or select **New Notification** to configure a new user notification. Refer to the User Notification Settings section in the [DocAve 6 Control Panel Reference Guide](#) for instructions on configuring user notification.

   You can click **View** to the drop-down list to view the detailed information of the selected user notification profile.

8. Click **Run** to start this job, or click **Cancel** to quit this operation. Click **Test Run** to run a test job first.

*Note: **Test Run** cannot be performed on the **Edit Group** function.

Breaking Inheritance for Sub-nodes

The **Break Inheritance for Sub-nodes** feature allows you to break permission inheritance to the sub-nodes under the selected node. This feature is supported on the site collection, site, list/library, and folder levels. To set up a plan for breaking permission inheritance for sub-nodes, complete the following steps:

1. Select a desired node, and click **Security** tab > **Stop Inheriting Permissions** > **Break Inheritance for Sub-Nodes**. The **Stop Inheriting Permissions** page appears.

2. Enter a **Plan Name**. A plan name with the format **Stop Inheriting Permissions HH:MM:SS YYYY-MM-DD** is provided by default.

   - Click **Check** to the plan name to check whether the specified plan name is available. A green check mark indicates that the specified plan name is available. A warning message appears if the specified plan name already exists and some suggested plan names are listed beneath.

   - Add an optional **Description**.

3. Select the sub-node that you want to **Stop Inheriting Permissions** from using the **Down to the … level** drop-down box. Permission inheritance from the currently-selected node to the specified sub-node is broken from their parent nodes.

4. Configure permissions for the nodes that will stop inheriting permissions.

   - **Copy Permissions from parent** –This option keeps the nodes' current permissions inheriting from parent nodes.

   - **Clear all permissions** – This option removes all of the nodes' current permissions.

5. Schedule Selection – Choose whether or not to use a schedule.

   - **No Schedule** – Run the plan without a schedule.

- **Configure the Schedule Myself** – Select this option to configure a customized schedule, and run the permission break by schedule. Fill in the parameters according to your desired schedule. After configuring the schedule for the plan, click **Calendar View** to view the scheduled search by day, week, or month.

6. Configure user **Notification** settings. Select a previously-created notification profile from the drop-down list, or select to create a New Notification. Refer to the User Notification Settings section in the [DocAve 6 Control Panel Reference Guide](#) for more information about creating a new notification.

   You can click **View** to the drop-down list to view the detailed information of the selected user notification profile.

7. Click **OK**. The plan is now available in **Plan Manager**. Alternatively, click **OK and Run Now** to run the job immediately. Access **Job Monitor** to view job details and download the job report.

Breaking Inheritance for Selected Node

The **Break Inheritance for Selected Node** feature allows you to break permission inheritance from the selected node's parent node. This feature is supported on the site, list/library, folder, and item levels. Follow the instructions below to break permission inheritance for the selected node.

Select a desired node, and click **Security** tab > **Stop Inheriting Permissions** > **Break Inheritance for Selected Node**. Then, in the new page, a message displays indicating that the changes will no longer affect the selected node if breaking permission inheritance. Click **OK** to confirm the operation.

When selecting **Break Inheritance for Selected Node**, DocAve will first copy the parent node's permission and then stop inheriting permissions from the parent node.

Pushing Inheritance to Sub-nodes

The **Push Inheritance to Sub-nodes** feature pushes the current selected node's permissions that are inherited from its parent down to sub-nodes. This feature is supported on the list/library and folder levels. To set up a plan for pushing inheritance to sub-nodes, complete the following steps:

1. Select a desired node, and click **Security** tab > **Inherit Permissions** > **Push Inheritance to Sub-Nodes**. The Inherit Permissions page appears.

2. Enter a **Plan Name**. A plan name with the format **Inherit Permissions HH:MM:SS YYYY-MM-DD** is provided by default.

   - Click **Check** to the plan name to check whether the specified plan name is available. A green check mark indicates that the specified plan name is available. A warning message appears if the specified plan name already exists and some suggested plan names are listed beneath.

   - Add an optional **Description**.

3. Select the nodes you want to **Inherit Permissions**.

- **Only current selection** – If selecting this option, only the current selected node will inherit permission from its parent node.

- **Down to the … level** – Selecting this option enables you to specify a sub-node; then, all nodes from the currently-selected node to the specified node will inherit permissions from their parent nodes after the job completes.

  o **Exclude current selection** – If enabling this option, the selected node does not inherit permission from its parent node.

4. **Schedule Selection** – Choose whether or not to use a schedule.

- **No Schedule** – Run the plan without a schedule.

- **Configure the Schedule Myself** – Select this option to configure a customized schedule, and run the permission inheritance by schedule. Fill in the parameters according to your desired schedule. After configuring the schedule for the plan, click **Calendar View** to view the scheduled search by day, week, or month.

5. Configure user **Notification** settings. Select a previously created notification profile from the drop-down list, or select to create a New Notification. Refer to the User Notification Settings section in the [DocAve 6 Control Panel Reference Guide](#) for more information about creating a new notification.

You can click **View** to the drop-down list to view the detailed information of the selected user notification profile.

6. Click **OK** and the plan is now available in **Plan Manager**. Or click **OK and Run Now** to run the job immediately. Access **Job Monitor** to view job details and download the job report.

Security Management Web Part

DocAve Administrator's Security Management Web part allows you to add, edit, delete, clone and search permissions for a site collection and the sites/lists/libraries under this site collection on a single page in SharePoint. To use this solution, you must first deploy the Security Management solution and enable the corresponding features in order to make the Security Management Web part available in the desired site collections.

Deploying the Security Management Solution

Refer to the steps below to deploy the DocAve Security Management solution to SharePoint 2010 or SharePoint 2013. Once you install and deploy the DocAve Security Management solution, the Security Management features will be listed in the site collection feature list.

To deploy the DocAve Security Management solution, complete the following steps:

1. Navigate to the **DocAve** tab > **Control Panel** > **Solution Manager**.

2. Select the target farm from the **Farm** drop-down list.

3. Select the **SP2010SecurityManagement.wsp** checkbox for a SharePoint 2010 environment or select the **SP2013SecurityManagement.wsp** checkbox for a SharePoint 2013 environment, and then click **Install** in the **Actions** group.

4. Once the solution is installed on the SharePoint farm, select the **SP2010SecurityManagement.wsp** checkbox or the **SP2013SecurityManagement.wsp** checkbox again and click **Deploy** in the **Actions** group.

   *Note: After deploying the **SP2013SecurityManagement.wsp** solution on a SharePoint 2013 farm, the feature cannot be activated on site collections using SharePoint 2010 experience version. To use the feature in the site collections using SharePoint 2010 experience version in a SharePoint farm, deploy the **SP2010SecurityManagement.wsp** solution to the Web applications where the specified site collections reside.

5. After the solutions are deployed successfully, the status of the solution is shown as **Deployed** in the **Status** column.

Refer to the **Solution Manager** section of the <u>DocAve 6 Control Panel Reference Guide</u> for information on performing more operations on solutions.

Activating the Security Management Features

Once the Security Management solution is deployed, the Security Management features must be activated on the desired site collections through SharePoint. To enable the Security Management features, complete the following steps:

1. In SharePoint, access the site collection on which you want to activate the Security Management Web part.

   - In SharePoint 2010, navigate to **Site Actions > Site Settings > Site collection features.** The **Site Collection Features** page appears.

   - In SharePoint 2013, navigate to the **Settings** icon ⚙ on the quick launch bar > **Site settings** > **Site collection features**. The **Site Collection Features** page appears.

2. Click **Activate** next to the following features. This enables the features for the selected site collection.

   - DocAve Security Management Feature

   - DocAve Security Management Ribbon

   - DocAve Security Search History Feature

   - DocAve Security Search Result Feature

3. After activating the Security Management features, the status of the feature reads **Active** in the **Status** column.

Using the Security Management Web Part

After completing the preliminary steps mentioned above, return to **Site Settings** (SharePoint 2010) or **Site settings** (SharePoint 2013) page of the desired site collection. A new link named **Security management** appears under the **Users and Permissions** gallery. Click the **Security management** link to access the Security Management Web part.

The tree structure of the site collection, the users, and the groups of each level (site collection, site and list/library) are displayed on the Security Management Web part interface.

All available actions (including **Grant Permissions**, **Edit User Permissions**, **Security Search**, and so on) are displayed on ribbon. Below is a screenshot of the Security Management Web part interface.
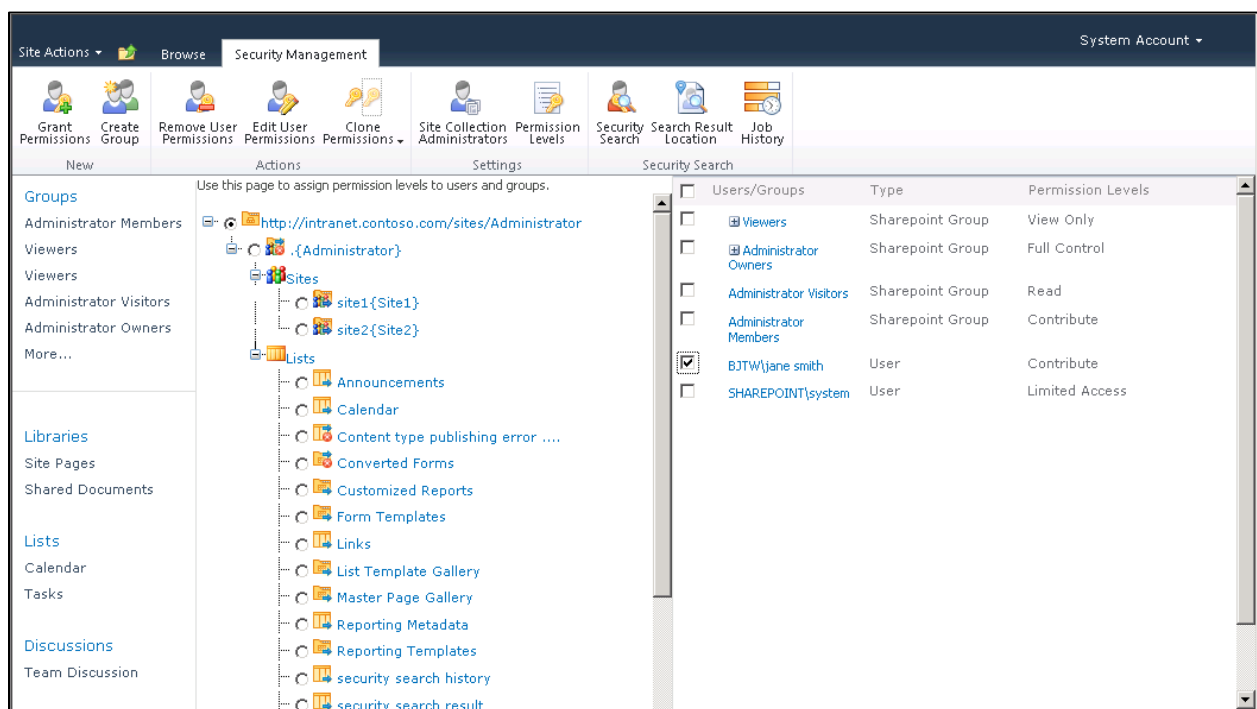
Figure 3: Security Management Web part interface.

The following functions in the Security Management Web part are unique functions of DocAve. SharePoint does not have such functions.

- Clone User Permissions – Refer to Cloning User Permissions for more information about this function.

- Clone Site Permissions – Refer to Cloning Site Permissions for more information about this function.

- Security Search – Refer to Performing a Security Search in Security Management Web Part for more information about this function.

- Search Result Location – Refer to Configuring Search Result Location for more information about this function.

- Job History – Refer to [Checking Security Search Job Status in the Security Management Web Part](#) for more information about this function.

Refer to the tables below for all functions provided by the Security Management Web part.

Functions on the site collection level:

Function	Location in SharePoint 2010	Location in SharePoint 2013
Grant Permissions	Login Site Collection > Site Actions > Site Settings > Site Permissions	Login Site Collection > Settings Icon ⚙ > Site settings > Site Permissions
Create Group	Login Site Collection > Site Actions > Site Settings > Site Permissions	Login Site Collection > Settings Icon ⚙ > Site settings > Site Permissions
Remove User Permissions	Login Site Collection > Site Actions > Site Settings > Site Permissions	Login Site Collection > Settings Icon ⚙ > Site settings > Site Permissions
Edit User Permissions	Login Site Collection > Site Actions > Site Settings > Site Permissions	Login Site Collection > Settings Icon ⚙ > Site settings > Site Permissions
Clone User Permissions	Login Site Collection > Site Actions > Site Settings > Security Management	Login Site Collection > Settings Icon ⚙ > Site settings > Security Management
Clone Site Permissions	Login Site Collection > Site Actions > Site Settings > Security Management	Login Site Collection > Settings Icon ⚙ > Site settings > Security Management
Site Collection Administrators	Login Site Collection > Site Actions > Site Settings > Site Permissions	Login Site Collection > Settings Icon ⚙ > Site settings > Site Permissions
Permission Levels	Login Site Collection > Site Actions > Site Settings > Site Permissions	Login Site Collection > Settings Icon ⚙ > Site settings > Site Permissions
Security Search	Login Site Collection > Site Actions > Site Settings > Security Management	Login Site Collection > Settings Icon ⚙ > Site settings > Security Management
Search Result Location	Login Site Collection > Site Actions > Site Settings > Security Management	Login Site Collection > Settings Icon ⚙ > Site settings > Security Management
Job History	Login Site Collection > Site Actions > Site Settings > Security Management	Login Site Collection > Settings Icon ⚙ > Site settings > Security Management

Functions on the site level:

Function	Location in SharePoint 2010	Location in SharePoint 2013
Grant Permissions	Login a Site > Site Actions > Site Settings > Site Permissions	Login a Site > Settings Icon ⚙ > Site settings > Site Permissions
Create Group	Login a Site > Site Actions > Site Settings > Site Permissions	Login a Site > Settings Icon ⚙ > Site settings > Site Permissions
Remove User Permissions	Login a Site > Site Actions > Site Settings > Site Permissions	Login a Site > Settings Icon ⚙ > Site settings > Site Permissions
Edit User Permissions	Login a Site > Site Actions > Site	Login a Site > Settings Icon ⚙ > Site

Function	Location in SharePoint 2010	Location in SharePoint 2013
	Settings > Site Permissions	settings > Site Permissions
Inherit Permissions\Stop inheriting Permissions	Login a Site > Site Actions > Site Settings > Site Permissions	Login a Site > Settings Icon ⚙ > Site settings > Site Permissions
Clone User Permissions	Login a Site > Site Actions > Site Settings > Security Management	Login a Site > Settings Icon ⚙ > Site settings > Security Management
Clone Site Permissions	Login a Site > Site Actions > Site Settings > Security Management	Login a Site > Settings Icon ⚙ > Site settings > Security Management
Permission Levels	Login a Site > Site Actions > Site Settings > Site Permissions	Login a Site > Settings Icon ⚙ > Site settings > Site Permissions
Security Search	Login a Site > Site Actions > Site Settings > Security Management	Login a Site > Settings Icon ⚙ > Site settings > Security Management
Search Result Location	Login a Site > Site Actions > Site Settings > Security Management	Login a Site > Settings Icon ⚙ > Site settings > Security Management
Job History	Login a Site > Site Actions > Site Settings > Security Management	Login a Site > Settings Icon ⚙ > Site settings > Security Management

Functions on the list/library level:

Function	Location in SharePoint 2010	Location in SharePoint 2013
Grant Permissions	Access a List/Library > List/Library > List/Library Permissions	Access a List/Library > List/Library > List/Library Permissions
Remove User Permissions	Access a List/Library > List/Library > List/Library Settings	Access a List/Library > List/Library > List/Library Settings
Edit User Permissions	Access a List/Library > List/Library > List/Library Settings	Access a List/Library > List/Library > List/Library Settings
Inherit Permissions\Stop inheriting Permissions	Access a List/Library > List/Library > List/Library Settings	Access a List/Library > List/Library > List/Library Settings
Clone User Permissions	Login the Site Collection or Site the List/Library resides in > Site Actions > Site Settings > Security Management	Login the Site Collection or Site the List/Library resides in > Settings Icon ⚙ > site Settings > Security Management
Clone Site Permissions	Login the Site Collection or Site the List/Library resides in > Site Actions > Site Settings > Security Management	Login the Site Collection or Site the List/Library resides in > Settings Icon ⚙ > site Settings > Security Management
Security Search	Login the Site Collection or Site the List/Library resides in > Site Actions > Site Settings > Security Management	Login the Site Collection or Site the List/Library resides in > Settings Icon ⚙ > site Settings > Security Management
Search Result Location	Login the Site Collection or Site the List/Library resides in > Site Actions > Site Settings > Security Management	Login the Site Collection or Site the List/Library resides in > Settings Icon ⚙ > site Settings > Security Management
Job History	Login the Site Collection or Site the List/Library resides in > Site	Login the Site Collection or Site the List/Library resides in > Settings Icon

Function	Location in SharePoint 2010	Location in SharePoint 2013
	Actions > Site Settings > Security Management	⚙ > site Settings > Security Management

Performing a Security Search in Security Management Web Part

Security Search enables you to search for users and groups, and the permissions of the specified users and groups, as well as the SharePoint objects that the users and groups have permissions to. To perform a security search in Security Management Web part, complete the following steps:

1. In the Security Management Web part, specify a search scope from the tree, and click **Security Search** on the ribbon.

2. Enter the name of the users or groups you want to search for in the **User/Group** text box. You can click the **Browse** icon to search desired users or groups using keywords, and click the **Check Names** icon to check whether the specified users or groups is available in your SharePoint environment. Separate each user or group with a semicolon. Add an optional description.

3. Configure the **Permission** settings to limit the users or contents searched according to the permissions assigned to them.

   - **Has Permissions** – Limit the search result based upon the permission; these include **Search for Any Permission**, **Full Control**, **Design**, **Contribute**, **Read**, **Limited Access**, and **View Only**.

   - **Exact permission** – Match the search result with the exact permission selected, while **Exact permission or better** matches the search result with users or content whose permission is no less than the selected permission.

   - **Include SharePoint users and groups with no permissions** – Select whether or not to search the SharePoint users and groups with no permissions. By default, they are excluded.

   - **Inherited Permission** – Search for the SharePoint objects with inherited permission in selected nodes.

   - **Explicit Permissions** – Search for the SharePoint objects with explicit permission in selected nodes.

4. Select a level for this security search in **Search Criteria** option. Only the SharePoint objects of the selected levels are included in the search result. The available levels for you to select are **Site collection**, **Site**, **List/Library**, **Folder** and **Item**.

5. By default, the **Search Result Location** is the current site collection has Security Management enabled. You can click the **Change Search Result Location** link to specify a new location under the current site collection for the security search job. Refer to the Configuring Search Result Location section for more information about the search result location.

6. Click **OK** to run the search job immediately, and it takes you to the **Security Search History** list where records the job status of the security search. Refer to Checking Security Search Job Status in the Security Management Web Part for more information about the **Security Search History** list.

Configuring Search Result Location

By default, security search results and security search history are created in the top-level site of the site collection that has the Security Management feature enabled. You can specify a new **Search Result Location** for security search jobs by clicking **Search Result Location** on the Security Management Web part ribbon, or clicking the **Change Search Result Location** link while configuring a security search job. The new location can only be a subsite in the site collection where the top-level site resides.

When running a security search job for the first time, a list named **Security Search Result** is generated in the configured **Search Result Location** automatically. After the **Security Search Result** list is created, all subsequent security search jobs that use this **Search Result Location** will store their search results in the same **Security Search Result** list. Each search job has its own folder in the **security search result** list, and the format of the folder name is: **Security SearchYYYY-MM-DD-HH-MM-SS**.

Checking Security Search Job Status in the Security Management Web Part

In the Security Management Web part, click **Job History** on the ribbon to access the **Security Search History** list. This list is automatically generated under the current site collection that has Security Management enabled while [Activating the Security Management Features](). All security search jobs are run within the current Security Management Web part, while corresponding job information is stored in the **Security Search History** list.

Monitoring and Controlling Actions and Changes in SharePoint

DocAve Policy Enforcer supports the ability to establish a limitation for certain actions and changes that have occurred in SharePoint environments. By applying the Policy Enforcer profiles including pre-configured rules and a source collection policy to the selected SharePoint nodes, Policy Enforcer keeps monitoring all actions and changes within your SharePoint environment. It can identify and generate a report of the out of policy objects. It also supports either automatically or manually fixing the issues. Policy Enforcer ensures that all of the actions and changes to your SharePoint environment remain within your organization's defined governance policy and under control. Refer to the topics below for information related to DocAve Policy Enforcer.

*Note: Policy Enforcer is supported for SharePoint 2010/2013 On-Premise and SharePoint Online.

Configuring the Policy Enforcer Database

In order to use Policy Enforcer, you must configure a dedicated Policy Enforcer database in SQL server for all of the farms within this DocAve platform. The Policy Enforcer database stores the all of the historical job data for Policy Enforcer.

*Note: To configure a Policy Enforcer database, you must be a member of the **Administrator** group.

To configure a Policy Enforcer database, complete the following steps:

1. Navigate to **DocAve 6** > **Administration** > **Administrato**r. Click the **Policy Enforcer** tab.

2. Click **Policy Enforcer Database** on the ribbon to configure a Policy Enforcer database. The **Policy Enforcer Database** window appears.

3. Configure the following settings for the database that will store Policy Enforcer job data:

   - **Configure Policy Enforcer Database –** Policy Enforcer supplies a default **Database server** and **Database name**. The database server of the DocAve 6 Control database is automatically set as the default database server for Policy Enforcer database. If desired, enter a new database server and database name in the corresponding fields. If the database does not exist, DocAve creates a database using the specified name. However, AvePoint recommends that you use the default database server for most instances.

   - **Authentication –** Specify the authentication mode, database credentials and an optional failover database server for the Policy Enforcer database:

     o Select the **Windows Authentication** or **SQL Authentication** mode for the database and specify the database credential for the selected authentication mode. After this, you can validate the specified account by clicking **Validation Test**.

- **Window Authentication (recommended)** – Use this method if you want the user's identity to be confirmed by Windows. Select a previously configured account from the **Managed account profile** drop-down list, or click **New Managed Account Profile** to create a new managed account profile in Control Panel. For more information on configuring a managed account profile, refer to the DocAve 6 Control Panel Reference Guide.

- **SQL Authentication** – SQL Server will confirm the user's identity according to the user's account and password.

   *Note: The specified account for creating or accessing the Policy Enforcer database must be the **db_creator** in the SQL server where you want to create the Policy Enforcer database and the **db_owner** in the newly created/existing Policy Enforcer database.

   o **Failover database server –** Optionally select this checkbox and specify a failover database server. In the event that the Policy Enforcer database collapses, the data stored in the Policy Enforcer database can be transferred to this standby database.

- **Advanced –**Click **Advanced** to specify a Policy Enforcer database by entering a connection string directly. Select the **Edit connection string directly** checkbox to activate this feature, and then enter the connection string according to the examples listed in the left pane.

4. Click **OK** to save the configurations.

Configuring the Source Collection Policy

Before creating the Policy Enforcer profile, you must configure the source collection policy to determine the data of which types of SharePoint events and/or conditions will be collected by Policy Enforcer. The Policy Enforcer rules use the collected data to identify whether the corresponding SharePoint events and conditions are within policy or out of policy.

To configure the source collection policy, complete the following steps:

1. Navigate to **DocAve 6** > **Administration** > **Administrator**.

2. On the **Policy Enforcer** tab, click **Source Management** on the ribbon to configure the auditing and scanning policy.

3. Click **Create** in the **Manage** group on the ribbon to create a new source collection policy.

4. In the **New Source Collection Policy** window, complete the following steps:

   a. **Source Collection Policy** – Enter the Policy Name, followed by an optional Description.

   b. Select **Auditor Mode** or **Scan Mode**, and then to select to enable or disable the corresponding event types for the selected mode.

- o **Auditor Mode** – Select the **Auditor Mode** checkbox and then complete the following configurations.
  - ▪ **Interval** – Specify how often this source collection mode will run to collect the Audit events of the enabled event types in SharePoint to identify out of policy objects. The collected data is stored as DocAve Job Data. Frequency of collection can improve quality of remediation but can impact SharePoint performance.
  - ▪ **Event Type** – By default, all of the event types are enabled to ensure all of the available audit events can be collected by DocAve to identify out of policy objects in SharePoint. To change the event types' statuses in this source collection policy, select the event types whose status you want to change, click **Disable** to disable the selected event types or click **Enable** to enable the event types. The Audit events of the disabled event types will not be collected by DocAve to identify out of policy objects.
- o **Scan Mode** – Select the **Scan Mode** checkbox and then complete the following configurations.
  - ▪ **Interval** – Specify how often this source collection mode will run to scan the conditions of the enabled event types in SharePoint to identify out of policy objects, settings, permissions and/or features. The collected data is stored as DocAve Job Data. Frequency of collection can improve quality of remediation but can impact SharePoint performance.
  - ▪ ***Note:** If "**Day(s)**" is selected as the **interval**, you can specify a start time for the jobs of this source collection mode.
  - ▪ **Event Type** – By default, all of the event types are enabled to ensure all of the available conditions can be collected by DocAve to identify out of policy objects in SharePoint. To change the event types' statuses in this source collection policy, select the event types whose statuses you want to change, click **Disable** to disable the selected event types or click **Enable** to enable the event types. The corresponding conditions of the disabled event types will not be collected by DocAve to identify out of policy objects.
- c. Click **Save** to save the configuration of the source collection policy.

After creating a new source collection policy, you can also make changes to the existing source collection policies in the **Policy Enforcer > Source Management** page:

- **Set as Default** – Select an existing policy and click **Set as Default** on the ribbon to set the selected policy as the default source collection policy for all of the Policy Enforcer profiles to be created.
- **Edit** – Select an existing policy and click **Edit** on the ribbon to edit this selected policy.
- **Delete** – Select one or more existing policies and click **Delete** on the ribbon to delete the selected policies permanently.

Configuring Policy Enforcer Profile

The Policy Enforcer profile manager integrates the configured source collection policies and the added rules that control the actions and changes in SharePoint. Once the added rules are activated and applied on the selected nodes, the corresponding actions and changes in SharePoint will be monitored by DocAve to identify out of policy objects. DocAve will report the violations with details and automatically adjust settings, permissions, and configurations or enable users to fix the issues manually if required.

Creating a Policy Enforcer Profile Using Profile Manager

To create the Policy Enforcer profile using Profile Manager, complete the following steps:

1. Navigate to **DocAve 6** > **Administration** > **Administrator**. On the **Policy Enforcer** tab, click **Profile Manager** on the ribbon to configure the Policy Enforcer profile.

2. Click **Create Profile** in the **Profile Management** group on the ribbon to enter the **Create Profile** page and then complete the following configurations:

   - **Profile Name** – Enter the profile **Name** and an optional **Description**.

   - **Scope** – Select a SharePoint on-premises farm or Registered SharePoint Sites group from the corresponding drop-down list as the scope where you want to apply this profile. Policy Enforcer will display the available rules in the **Add Rule** window based on the scope you select here. Refer to Appendix G: Supported List of Policy Enforcer Rules for SharePoint On-premises and SharePoint Online for the supported condition of Policy Enforcer rules for SharePoint on-premises farms and SharePoint Online site collections.

   - **Agent Group** – Select a production Agent group from the drop-down list to execute the jobs for this profile. An Agent group can utilize multiple Agents for loading balancing and performance improvement.

   - **Rules** – Click **Add Rule** below the **Rules** table or on the ribbon to add rules to this profile. All of the available rules for the scope selected above are displayed in the pop-up **Add Rule** window. Select the checkboxes of the rules that you want to apply on the selected scope and click **OK** to add the selected rules to this profile. You can view the added rules in the **Rules** table and click a specified rule name to configure the rule. For detailed information on configuring a rule, refer to Managing Rules in Policy Enforcer Profile in this guide.

     *Note: You must activate at least one rule for a profile, and you must configure all of the active rules in the profile.

   - **Source Collection Policy** –Select one of the previously-configured source collection policies for the event types to be monitored by Policy Enforcer from the drop-down list, or select New Source Collection Policy to create a new one. If a policy has not been configured yet, refer to Configuring the Source Collection Policy for details.

     o **View** – After selecting a policy from the drop-down list, click **View** to view details about the selected source collection policy.

- **Retention Policy** – Specify the retention period by entering a positive integer and selecting **Day(s)**, **Week(s)**, or **Month(s)** for keeping the job data associated with this profile.

- **Send Periodic Reports** – Select the **Send periodic reports to the recipients configured in each rule** checkbox to send daily or weekly reports for the violations of each rule in this profile to the recipient configured in the corresponding rule and then configure the frequency for the periodic reports:

    o **Send daily reports at …**– To send daily reports, click this radio button and then configure when to send the report every day by selecting a time from the drop-down list.

    o **Send weekly reports every … at …**– To send weekly reports, click this radio button and then configure when to send the report every week by selecting the day of the week and the time of the day from the drop-down lists.

3. Click **Save** in the **Commit** group to save the configuration of this profile. The **Profile Manager** page appears.

4. The created profile is displayed in the **Profile Manager** page. To manage these created profiles in **Profile Manager**, refer to Managing Existing Policy Enforcer Profiles .

Managing Existing Policy Enforcer Profiles

After creating a new Policy Enforcer profile, you can manage the existing profiles in the **Profile Manager** page. Select the checkbox to the left of the profile name and choose one of the following buttons on the ribbon:

- **View Details** – Click **View Details** to view the rules and settings in the selected profile in the **Profile Details** page.

- **Edit** – Click **Edit** to edit the selected profile in the **Edit Profile** page. For details on editing the rules and settings of the profile, refer to Creating a Policy Enforcer Profile Using Profile Manager. After finish editing the profile, click **Save** > **Save** or **Save and Run Now** to save the changes.

    o Click **Save** > **Save** to save changes to the profile and return to the **Profile Manager** page.

    o If you edit an existing Policy Enforcer profile which has been applied on some nodes of the SharePoint farm, click **Save** > **Save and Run Now** to save the changes to the profile and run this job immediately.

      *Note: **Save** > **Save and Run Now** is only available when you edit a profile which has been applied to specific SharePoint nodes.

- **Delete** – Click **Delete** on the ribbon to permanently delete an existing profile selected in the Policy Enforcer Profile field after expanding the SharePoint farm.

*Note: You cannot delete a profile when it is still applied to SharePoint nodes. It is recommended that you use the **Profile Scope** feature to discover where this profile is applied and remove it first.

- **Profile Scope** – Click **Profile Scope** to view all of the SharePoint scopes where Policy Enforcer profiles have been applied. You can also remove the applied profiles from SharePoint scopes with the **Remove Profile** feature. Select the scopes and click **Remove Profile** to remove the applied profiles from the selected scopes. Once the profiles are removed, they will no longer be applied on the specific SharePoint nodes.

Managing Rules in Policy Enforcer Profile

In the **Create Profile/ Edit Profile/Create or Apply Profile** page, configure a Policy Enforcer rule or perform other operations to manage the previously added rules for a particular profile.

Configuring a Policy Enforcer Rule

After adding a rule to a Policy Enforcer profile, you must configure the required settings for this rule in the **Configure Rule** window. To configure a particular Policy Enforcer rule, complete the following steps:

1. Select the checkbox of the desired rule in the **Rules** table.

2. Click **Configure Rule** on the ribbon, or click the link of the desired rule name in the **Rule** table. The **Configure Rule** window appears.

3. To configure the selected rule in the **Configure Rule** window, complete the following settings:

    a. **Rule Summary** – In the **Rule Summary** field, the name, description and affected event type of this selected rule will be displayed.

    b. **Rule Parameters** – In this section, each rule provide you with its specific parameters based on the event type it monitors. Configure the specified parameters to customize each Policy Enforcer rule. The settings configured with these parameters will be used as the standard by DocAve to identify the violations in SharePoint. Any actions and conditions in SharePoint do not comply with the configured standard will be identified as out of policy.

    c. **Filter Policy** – Select a previously created filter policy from the **Filter Policy** drop-down **list**. A filter policy allows you to apply this rule using certain conditions. Refer to the Configuring Filter Policies section in the *DocAve 6 Control Panel Reference Guide* for more information on creating a new filter policy.

    d. **Custom Action** – Select the checkbox on the right site to perform automatic actions on the violations once DocAve identifies out of policy objects, settings and/or permissions based on the settings defined in the rule. For example, the out of policy files will be deleted to the site level recycle bin and the out of policy settings will be reverted to the states defined in the rule. If this option is unselected, DocAve will not take action on the violations.

e. **Recipient** – Specify the users who will receive e-mail notifications for the violations of this rule.

- **Recipient** – Use the people picker to specify the Active Directory users or Form-Based Authentication (FBA) users who will receive an e-mail notification report of the violations of this rule.

- **Include the site collection administrator** – Select this option to deliver the e-mail notification of the violations to the site collection administrators.

- **Include the users who violate this rule** – Select this option to notify the end-users who violate the specified rule of their out of policy operations. Note that this option is only available for those rules of Auditor Mode event types.

  *Note: Before configuring the **Notification** settings, you must make sure the **Outgoing E-mail** settings have been configured in **Control Panel**. For detailed information on configuring the Outgoing E-mail settings, refer to the [DocAve 6 Control Panel Reference Guide](#).

f. **Send Notification Immediately** – Select whether to send notifications to the **recipients** configured above immediately when Policy Enforcer identifies any violations of this rule.

4. Click **OK** to save the configurations of this rule.

In the **Create Profile/ Edit Profile/Create or Apply Profile** page, you can also perform the following operations on the rules of the currently configured profile:

- **Remove Rule** – To remove the previously added rules from the currently configured profile, select the checkboxes of the corresponding rules in the **Rules** table, and click **Remove Rule** on the ribbon.

- **Activate** – Select the checkboxes of the added rules in the **Rules** table, and click **Activate** on the ribbon to activate the rules.

- **Deactivate** – Select the checkboxes of the added rules which are already activated in the **Rules** table, and click **Deactivate** on the ribbon to deactivate the rules. When the rules are deactivated, the actions and conditions that are related to the deactivated rules will not be monitored by Policy Enforcer when running the jobs of this profile.

Customizing Rules with Policy Enforcer SDK

DocAve Policy Enforcer implements a set of APIs that allow you to customize Policy Enforcer rules by calling Policy Enforcer APIs. Refer to the Policy Enforcer SDK Help file **AgentCommonPolicyEnforcerAPI.chm** for more information on using Policy Enforcer APIs. This file is located in the DocAve Agent installation path, which is *…\AvePoint\DocAve6\Agent\Documents\SDK\ Administrator* by default.

Applying a Policy Enforcer Profile

After creating the Policy Enforcer profiles, you can apply them on the selected nodes of the SharePoint farm. When the profile is applied on the selected nodes, DocAve will start to audit the actions and scan the settings on the specified nodes. To apply a profile to one or more nodes in SharePoint, complete the following steps:

1. Navigate to **DocAve 6** > **Administration** > **Administrator**.

2. On the **Policy Enforcer** tab, expand the farm tree in the **Scope** field and select one or more nodes (from the farm level to the site level) where you want to apply the profile and click **Create or Apply Profile** on the ribbon to enter the **Create or Apply Profile** page.

3. View the message bar on the top of the **Create or Apply Profile** area or a pop-up window to display these details about the applied profiles for the selected nodes.

    - When you select one node in the scope tree:
        - If there is no profile applied on this node, a message bar appears on the top of the **Create or Apply Profile** area. This message informs that you can choose a desired option from the **Profile Name** section to apply a profile to this node.
        - If there is a profile applied on this node, the currently applied profile's name is displayed in the message bar. You can perform the following operations:
            - To edit the currently applied profile, click **Edit** and enter the profile in the **Edit Profile** page. For the detailed information on editing a Policy Enforcer profile, refer to the section <u>Configuring Policy Enforcer Profile.</u>
            - To apply a new profile to this node, select a desired option from the **Profile Name** section.
        - If this node is inheriting rules from its parent node, the inherited profile's name is displayed in the message bar. You can perform the following operations:
            - To edit the inherited profile, click **Edit** and edit the profile in the **Edit Profile** page. Changes you make in this page will affect the parent node and all its sub nodes which are inheriting the rules and settings.
            - To apply a unique profile to this node, click **Stop Inheriting** to stop inheriting the rules and settings from the parent node and then choose a desired option from the **Profile Name** section to apply a new profile to this node.

                *Note: After you break a particular node's profile inheritance, use the **Inherit** button to make it inherit the profile from its parent again. For detailed information on the **Stop Inheriting** and **Inherit** operations, refer to <u>Inheriting and Stopping Inheriting</u>.
    - When you select more than one node in the scope tree:
        - If there is no profile applied on the selected nodes, a message bar appears on the top of the **Create or Apply Profile** area. This message says you can choose a

desired option from the **Profile Name** section to create or apply a new profile for the selected nodes.

- o If any of the selected nodes has a profile applied or is inheriting rules from a parent node, a pop-up window appears to display the profile applied status of the selected nodes. In this window, you can view the current profile or inherited profile on each selected node and then select whether apply another profile to these nodes in bulk.

  - To apply a new profile to the selected nodes in bulk, click **Proceed Anyway** to access the **Create or Apply Profile** page and then choose a desired option from the **Profile Name** section to create or apply a new profile for the selected nodes.

  - To stop the profile inheritance or apply profile inheritance to the selected nodes in bulk, refer to Inheriting and Stopping Inheriting.

  - If you do not want to make any changes to the selected nodes in bulk, click **Cancel** to exit the **Create or Apply Profile** interface.

4. In the **Create or Apply Profile** area, configure the following settings:

- **Profile Name** – Select one of the following radio buttons to apply a profile to the selected nodes in the scope tree:

  - o To reuse an existing profile, select **Reuse an existing profile** and select a profile from the drop-down list. This option expands the scope of the original profile. Select this option to reuse an existing profile in a different scope.

    *Note: The rules and settings in the existing profile cannot be modified from this screen.

  - o To create a new profile based on an existing profile, select **Configure new rules and settings based on an existing profile** and select an existing profile to copy from the drop-down list. Use this selection to modify the rules and settings of an existing profile and save the modification as a new one with a different profile name. For the detailed information on modifying a Policy Enforcer profile, refer to the section Configuring Policy Enforcer Profile.

  - o To create a new profile with new rules and settings, select **Create my own rules and settings** and start to configure the rules and settings for a new profile. For the detailed information on configuring a Policy Enforcer profile, refer to the section Configuring Policy Enforcer Profile.

- **Agent Group** – Select a production Agent group from the drop-down list to execute the jobs for this profile. An Agent group can utilize multiple Agents for loading balancing and performance improvement.

- **Rules** – Click **Add Rule** below the **Rules** table or on the ribbon to add rules into this profile. All of the available rules for the selected scope are displayed in the pop-up **Add Rule** window. Select the checkboxes of the rules that you want to apply on the selected scopes and click **OK** to add the selected rules to this profile. You can view the added

rules in the **Rules** table and click a specified rule name to configure the rule. For detailed information on configuring a rule, refer to [Managing Rules in Policy Enforcer Profile](#).

*Note: You must activate at least one rule for each profile. You cannot save a profile with no active rules.

- **Source Collection Policy** – Select one of the previously-configured source collection policies for the event types to be monitored by Policy Enforcer from the drop-down list, or select New Source Collection Policy to create a new one. If a policy has not been configured yet, refer to [Configuring the Source Collection Policy](#) for details.

  o **View** – After selecting a policy from the drop-down list, click **View** to view details about the selected source collection policy.

- **Retention Policy** – Specify the retention period by entering a positive integer and selecting **Day(s)**, **Week(s)**, or **Month(s)** for keeping the job data associated with this profile.

- **Send Periodic Reports** – Select the **Send periodic reports to the recipients configured in each rule** checkbox to send daily or weekly reports for the violations of each rule in this profile to the recipient configured in the corresponding rule and then configure the frequency for the periodic reports:

  o **Send daily reports at …**– To send daily reports, click this radio button and then configure when to send the report every day by selecting a time from the drop-down list.

  o **Send weekly reports every … at …**– To send weekly reports, click this radio button and then configure when to send the report every week by selecting the day of the week and the time of the day from the drop-down lists.

5. After completing the configuration of a profile, click **Apply** > **Apply** or **Apply** > **Apply and Run Now** to apply the profile to the selected nodes. If you have selected more than one node in the scope tree, and some of the selected nodes already have a profiles applied to them or are inheriting rules from a parent nodes, you must configure the conflict resolution in the pop-up window before applying the profile in bulk. For the detailed information on configuring the conflict resolution, refer to [Configuring Conflict Resolution](#).

- Click **Apply** > **Apply** on the ribbon to apply the rules and settings to the selected nodes of the SharePoint farm. The applied profile will be displayed in the **Scheduled Job Monitor** page. Policy Enforcer will start the jobs to scan SharePoint after one interval configured for the Auditor Mode or Scan Mode in this profile's source collection policy. If "**Day(s)**" is selected as the **interval** for the Scan Mode, Policy Enforcer will start the jobs of Scan Mode rules at the specified start time.

- Click **Apply** > **Apply and Run Now** on the ribbon to apply the profile to the selected nodes of the SharePoint farm and run the job immediately.

*Note: The Policy Enforcer jobs associated with the rules of Auditor Mode or Scan Mode are based on their respective intervals configured in the corresponding source collection mode. That is to say, the same profile might run the jobs of Auditor Mode rules and Scan Mode rules based on two different intervals.

Inheriting and Stopping Inheriting

After applying a Policy Enforcer profile to a particular node, the sub-nodes automatically inherit the rules in the profile applied to their parent node.

When applying profiles for the first time, you can apply profiles directly at any level that Policy Enforcer supports (the farm/Web application/site collection/site level). After one profile has been applied to a node at particular level (Level A), you can still apply a profile directly to the nodes at levels that are higher than Level A. However, if you want to apply a profile to a node at a level that is lower than Level A, you must first break the node's inheritance from its parent node.

Refer to the sections below for details instructions on stopping inheriting profiles from parent nodes and inheriting profiles again.

Stopping Inheriting Profiles

Refer to the section below to stop inheriting profiles from parent nodes.

Stopping Inheriting a Profile When Selecting One Node on the Tree

If you select a node on the tree and the selected node is currently inheriting a profile from its parent node, complete the following steps to break the profile inheritance of the selected node:

1. Select the desired node on the tree and click **Create or Apply Profile** on the ribbon. A message bar appears on the top of the **Create or Apply Profile** area. This message informs that the selected node is currently inheriting a profile from its parent node and the inherited profile's name is also displayed in the message bar.

2. Click **Stop Inheriting** on the ribbon.

3. Click **OK** in the pop-up window.

*Note: Once the selected node stops inheriting the profile from its parent node, the rules and settings in the previously inherited profile are removed from this node. The changes of the profile applied on the parent node will not affect this node.

Stopping Inheriting a Profile When Selecting Multiple Nodes on the Tree

If you select multiple nodes on the tree and some of the selected nodes are currently inheriting profiles from parent nodes, complete the following steps to break the profile inheritance of these nodes:

1. Select the desired nodes on the tree and click **Create or Apply Profile** on the ribbon. If some of the selected nodes are inheriting profiles from parent nodes or already have profiles applied to them , a pop-up window appears to display the profile applied status of the selected nodes.

2. Click **Proceed Anyway** to access the **Create or Apply Profile** page.

3. Click **Stop Inheriting** on the ribbon.

4. Click **OK** in the pop-up window.

*Note: Once the selected nodes stop inheriting the profile from parent nodes, the rules and settings in previously inherited profiles are removed from these nodes. The changes of the profiles applied on the parent nodes will not affect these nodes.

*Note: The **Stop Inheriting** action does not affect the selected nodes in the following situations:

- The node whose profile inheritance has already been broken.
- The node whose parent node has never been applied a profile.

Inheriting Profiles from Parent Nodes

If you have broken the profile inheritance on some particular nodes, you can inherit the profiles from their parent nodes again.

Inheriting Profiles from a Parent Node When Selecting One Node

If you select a node on the tree and the selected node has broken the profile inheritance from its parent node, complete the following steps to inherit the profile from the parent node again:

1. Select the desired node on the tree and click **Create or Apply Profile** on the ribbon.
2. Click **Inherit** on the ribbon.
3. Click **OK** in the pop-up window.

*Note: Once the selected node inherits a profile from its parent node again, the currently applied profile will be overwritten by the profile applied to its parent node.

Inheriting Profiles from a Parent Node When Selecting Multiple Nodes

If you select multiple nodes on the tree and some of the selected nodes are currently inheriting profiles from parent nodes, complete the following steps to break the profile inheritance of these nodes:

1. Select the desired nodes on the tree and click **Create or Apply Profile** on the ribbon. If some of the selected nodes are inheriting profiles from parent nodes or already have profiles applied to them, a pop-up window appears to display the profile applied status of the selected nodes.
2. Click **Proceed Anyway** to access the **Create or Apply Profile** page.
3. Click **Inherit** on the ribbon.
4. Click **OK** in the pop-up window.

*Note: Once you perform the **Inherit** action on the selected nodes, the selected nodes will inherit the profiles applied to their parent nodes again and the currently applied profiles will be overwritten.

*Note: The **Inherit** action does not affect the selected nodes in the following situations:

- The node currently inheriting a profile from its parent node.
- The node whose parent node has never been applied a profile.

Configuring Conflict Resolution

When some of the selected nodes in the **Create or Apply Profile** page already have a profile applied to them or are inheriting rules from a parent node, you must select a conflict resolution for these nodes to handle the conflict before applying a profile in bulk. To configure a conflict resolution for a conflicting node, view this node's profile applied status in the **Current Profile** and **Inherited Profile** columns and then select an option in the **Conflict Resolution** column:

- **Overwrite** – The newly applied profile will overwrite the currently applied profile in place. For those nodes which do not have a **Current Profile** or **Inherited Profile**, the current configured profile will be applied to them.

- **Skip** – Keep the rules and settings applied by the current profile to this node in place. The new profile will not be applied to the selected node. For those nodes which do not have a **Current Profile** or **Inherited Profile**, the current configured profile will not be applied to them.

Click **OK** to save the configuration and start to apply the new profile to the selected nodes, or click **Cancel** to return to the **Create or Apply Profile** page without saving the conflict resolution and applying the profile.

Generating a Report of the Policy Enforcer Profile

After the job of the profile completes, all of the out of policy actions and changes are recorded as the job data of the specified profile. Policy Enforcer enables you to generate a report based on the latest event data for the selected SharePoint nodes. The report displays the SharePoint nodes where out of policy objects, permissions, and settings reside with the details of the rules and violations. It also supports to fix the violations with the Custom Actions configured in the corresponding rules or perform manual operations to fix the violations if desired.

To generate the report of the Policy Enforcer profile, complete the following steps:

1. Navigate to **DocAve 6** > **Administration** > **Administrator**.

2. On the **Policy Enforcer** tab, expand the farm tree in the **Scope** field and select the nodes that the job of the Policy Enforcer profiles have been performed on.

3. Click **Generate Report** on the ribbon to generate the report of the latest data related to the Policy Enforcer profile of the selected nodes.

4. In the **Generate Report** page. If the selected scope is within policy, the **Status** column is marked with a checkmark ( ). If the rule has been violated, the **Status** column is marked with a cross mark ( ). Click the profile name to view the rules which have been applied to the specified scope. Click the information icon ( ) on the right of each rule name to view the more information about the rule.

5. You can click the rule name to display the SharePoint nodes including the out of policy objects, permissions, settings or features. If desired, refer to the **Status** column of each row to perform manual operations to fix the violations.

- **Fixed automatically** – Violations have been fixed automatically by Policy Enforcer based on the Custom Action configured in the rules.

- **Can be fixed** – Custom Action Settings of the specified rules are turned off. Policy Enforcer has not taken action on the violations. You can choose to fix the violations in bulk based on the Custom Action configured in the rules by selecting the nodes and clicking **Fix** on the ribbon.

- **Requires manual operation** – Policy Enforcer does not support to automatically fix the specified violations based on the Custom Action configured in the rules. The rule **Move** and **Copy** do not support the **Custom Action Settings** feature. You need to fix the violations with manual operations. To fix the violations manually, select the corresponding nodes and click **Manual Operation Required** on the ribbon or the manual operation ( ) button in the **Action** column to trim down to the out of policy nodes in the DocAve tree in the **Management** page of Administrator. You can manually reconfigure the settings to fix the violations in this node if desired.

- **Error** – An error occurred while fixing the violations by Policy Enforcer based on the Custom Action configured in the rules. Refer to the exception details listed below the node's name and then select operations to fix the issue accordingly. Or contact your SharePoint administrator for detailed information.

6. To view the detail information for the violations in a specific out of policy node under a rule name, click the node. The detail information for the violations of the specific rule in this node will be displayed below.

7. To export the report, click **Export** on the ribbon to configure the export settings in the pop-up window.

- **Report Format** – Select a report type from the drop-down list.

- **Export Settings** – Select an export location type for storing the report.

  o **Export to local immediately** – Select this option to export the report to the local file system location of the currently used server.

  o **Offline export** – Select this option to export the report to the location on the specified server. When selecting this option, the following settings are displayed as the further configuration.

    ▪ **Export Location** – Select an existing export location from the drop-down box to store the report before exporting.

    ▪ **E-mail Notification** – Select an existing notification profile from the drop-down box. A notification e-mail will deliver to the users who export the report.

After the configuration of the settings above, click **OK** to start the export operation.

*Note: By default, for performance reasons, DocAve only displays the first 2000 nodes which contain an object that is not within policy. To view all of the out-of-policy nodes and their objects, you can either generate an export report or increase the display limit within the DocAve configuration file. To increase the display limit, modify the **CAPolicyEnforcerViolationNodeQuotas** property located in the configuration file at the following DocAve install path: *\AvePoint\DocAve6\Manager\Control\Config\CentralAdmin\CentralAdminWebUtility.config*.

Hiding Out-of-Policy Nodes from the Generate Report

If you do not want to handle all of the out-of-policy nodes in the **Generate Report** page immediately, you can hide the out-of-policy nodes you want to dispose later for a specific period by using the **Hide** function. The hidden nodes will be hidden from the report of this rule and kept in the **Hidden List** until the expiration date.

To hide an out-of-policy node from the **Generate Report** page, complete the following steps:

1. Select the out-of-policy node you want to hide by selecting the corresponding checkbox.

2. Click **Hide** on the ribbon, and select an expiration period for hiding the selected node.

   This node disappears from the **Generate Report** page and is kept in the **Hidden List**.

2. Go to the **Hidden List** to view and manage all of the hidden out-of-policy nodes.

Managing Hidden Out-of-Policy Nodes

Click **Hidden List** on the ribbon. The **Hidden Issues** window appears. You can view and manage all of the hidden out-of-policy nodes on this window.

Viewing Hidden Out-of-Policy Nodes

In the **Hidden Issues** window, review the following information for a specific out-of-policy node:

- **Rule Name** – The rule which has been violated in this node.

- **Profile Name** – The profile to which the violated rule belongs.

- **URL** – The URL of this node.

- **Hidden Date** – The date when this node is hidden.

- **Expiration Date**– The date when the hiding action expires and this node will appear on the **Generate Report** page again.

- **Details** – The detailed information of the out-of-policy operations or settings in this node.

Changing Expiration Date

To change the date expiration for hiding out-of-policy nodes, complete the following steps:

1. Select the nodes you want to change by selecting their corresponding checkboxes.

2. Click **Change Expiration Date** on the ribbon. The window for changing the expiration date appears.

3. Click the calendar button and select your desired date as the new expiration date for the selected nodes.

4. Click **OK** to save the change, and return to the **Hidden Issues** interface.

Unhiding Out-of-Policy Nodes

To unhide specific hidden out-of-policy nodes and make them visible on the **Generate Report** page again, complete the following steps:

1. Select the nodes which you want to unhide by selecting the corresponding checkboxes.

2. Click **Unhide** on the ribbon.

3. Once a specific node is unhidden, you can view this node on the **Generate Report** page again.

Downloading Search Reports

Read the following sections for information on downloading admin and security search reports.

Downloading Admin Search Reports

To download an admin search report, complete the following steps:

1. After performing an admin search, access **Job Monitor**.

2. After the search completes, access the **Download Result** page for downloading the report in either of the following two methods:

    *   To access the **Download Result** page from **Job Monitor** directly, select the desired job, and click **Download Report** in the **Tools** group on the ribbon. The **Download Result** window appears.

    *   To access the **Download Result** page from the **Download Report** page, complete the following steps:

        i.   Select the desired job and click **Search Result** in the **Tools** group on the ribbon. The **Download Report** page appears.

        ii. Click **Download Report** on the ribbon. The **Download Result** window appears.

3. In the **Download Result** page, refer to Downloading Reports in the Download Result Page for detailed instructions on downloading the report.

Downloading Security Search Reports

To download a security search report, complete the following steps:

1. After performing an admin search access **Job Monitor**.

2. After the search completes, access the **Download Result** page for downloading the report in either of the following two methods:

    *   To access the **Download Result** page from **Job Monitor** directly, select the desired job, and click **Download Report** in the **Tools** group on the ribbon. The **Download Result** window appears.

    *   To access the **Download Result** page from the **Search Result Tools** page, complete the following steps:

        i.   Select the desired job and click **Search Result** in the **Tools** group on the ribbon. The **Search Result Tools** page appears.

      ii.   Click **Download Report** on the ribbon. The **Download Result** window appears.

3. In the **Download Result** page, refer to [Downloading Reports in the Download Result Page](#) for detailed instructions on downloading the report.

Downloading Reports in the Download Result Page

To download a report in the **Download Result** page, complete the following steps:

1. **Result Format** – Select a report type from corresponding drop-down box.

2. **Download Settings** – Select a downloading location type for storing the report.

   - **Export to local immediately** – Select this option to download the report to the local file system location of the currently used server.

   - **Offline export** – Select this option to download the report to the location on the specified server. When selecting this option, the following settings are displayed as the further configuration.

     o **Export Location** – Select an existing export location from the drop-down box to store the report before downloading.

     o **Notification** – Select an existing notification profile from the drop-down box. A notification e-mail will deliver to the users who download the report.

3. After the configuration of the settings above, click **OK** to start the download operation.

Administrator for SharePoint Online

You can use Administrator to manage your SharePoint Online site collections. To perform the Administrator functions on your SharePoint Online site collections properly, you must configure your **Agent Groups** and **Register SharePoint Sites** in **Control Panel**. For more detailed information about this configuration, refer to the [DocAve 6 Control Panel Reference Guide.](#)

For supported and unsupported functions for SharePoint Online, refer to [Appendix F: Supported and Unsupported List of DocAve Administrator Functions for SharePoint Online](#).

Administrator Caveats

In DocAve Administrator, the People Picker (Check Names icon) does not support checking CA SiteMinder-certificated users by default. Contact [AvePoint Support](#) if you want to make CA SiteMinder-certificated users able to be checked by DocAve People Picker.

Using Hot Key Mode

In order to work faster and improve your productivity, DocAve supports hot key mode for you to perform corresponding actions quickly by only using your keyboard. To access hot key mode from the Administrator interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard.

The following table provides a list of hot keys for the **Administrator** tab. To return to the top level after accessing a lower-level interface, press **Ctrl** + **Alt** + **Z** on your keyboard. For example, continuing pressing **H** to jump to the Administrator **Home** page.

Operation Interface	Hot Key
Management	M
Configuration	J
Security	S
Search Result Tools (for **Security Search**)	R
Export Settings	E
Policy Enforcer	F
Plan Manager	P
DocAve Home Page	1
AvePoint Official Website	2
Control Panel	3
Job Monitor	4
Plan Group	5
Health Analyzer	6
Account Information	9
Help and About	0

Management Tab

Operation and Hot Key			
Farm Level			
New		N	
Admin Search	S	Admin Search Wizard Mode	A
		Admin Search Form Mode	B
		Start with a Predefined Search	C
Farm Management	M	Manage Farm Features	A
		Manage Farm Solutions	B
		Manage User Solutions	C
Servers in Farm		F	
Services on Server		O	
Quiesce Farm		Q	
Service Applications	A	Manage Service Applications	M
Search Service (hidden when specifying the	V	File Types	F
		Server Name Mappings	S

Operation and Hot Key			
SharePoint 2013 farm)		Authoritative Pages	A
Default Database Server		D	
Data Retrieval Service		R	
Specify Quota Templates		T	
SharePoint Farm Summary	U	Review Database Status	D
		Check Product and Patch Installation Status	E
Search Duplicate Files		H	
Job Monitor		J	
Web Application Level			
New	N	New Site Collection	S
		New Content Database	D
Extend		X	
Delete	D	Delete Web Application	D
		Remove SharePoint from IIS Web Site	R
Admin Search	S	Admin Search Wizard Mode	A
		Admin Search Form Mode	B
		Start with a Predefined Search	C
General Settings	G	General Settings	G
		Resource Throttling	R
		Workflow	W
		Outgoing Email	O
		Mobile Account	M
Site Use and Deletions		U	
Manage Features		F	
Manage Paths		P	
Service Connections		C	
Manage Content Database		M	
Site Collection List		L	
Delete Orphan Sites		O	
Search Web Parts		W	
Search Duplicate Files		H	
Job Monitor		J	
Site Collection Level			
New		N	
Move		M	
Delete		D	
Admin Search	S	Admin Search Wizard Mode	A
		Admin Search Form Mode	B
		Start with a Predefined Search	C
Site Collection Features		F	
Portal Site Connection		P	
Content Type Publishing		C	
Web Part		E	
Themes		T	

Operation and Hot Key			
Solutions	U		
Site Columns	L		
Check Broken Link	B		
Search Web Parts	W		
Search Duplicate Files	H		
Job Monitor	J		
Sub-site Level			
New	N	New Subsite	S
		New List/Library	L
Delete		D	
Admin Search	S	Admin Search Wizard Mode	A
		Admin Search Form Mode	B
		Start with a Predefined Search	C
Site Features	F		
Reset to Site Definition	E		
Regional Settings	R		
Site Columns	L		
Site Content Types	T		
Master Page	M		
Check Broken Link	B		
Search Web Parts	W		
Search Duplicate Files	H		
Job Monitor	J		
List/Library Level			
New Folder	N		
Delete	D		
Admin Search	S	Admin Search Wizard Mode	A
		Admin Search Form Mode	B
		Start with a Predefined Search	C
No Checked In Version Files	C		
Workflow Settings	W		
Metadata and Keywords Settings	M		
Information Management Policy Settings	P		
Indexed Columns	I		
Job Monitor	J		
Folder Level			
New Folder	N		
Delete	D		
Admin Search	S	Admin Search Wizard Mode	A
		Admin Search Form Mode	B
		Start with a Predefined Search	C
View Properties	V	Edit	E
Job Monitor	J		
Item Level			
Delete	D		

Operation and Hot Key			
Admin Search	S	Admin Search Wizard Mode	A
		Admin Search Form Mode	B
		Start with a Predefined Search	C
Job Monitor		J	

Admin Search Wizard Mode/Delete Orphan Sites

Operation		Hot Key	
Back		B	
Next		N	
Finish	F	Finish and Run Now	R
		Finish	F
Cancel		C	

Search Web Parts/Search Duplicate Files

Operation		Hot Key	
OK	S	OK and Run Now	R
		OK	S
Cancel		C	

Configuration Tab

Operation and Hot Key			
Farm Level			
E-mail and Text Message(SMS)	E	Configure Outgoing E-mail Settings	A
		Configure Incoming E-mail Settings	B
		Configure Mobile Account	C
Alternate Access Mappings		A	
Privacy Options		O	
Cross-Firewall Access Zone		Z	
Records Center		R	
InfoPath Forms Services	I	Manage Form Templates	A
		Configure InfoPath Forms Services	B
		Upload Form Template	C
		Manage Data Connection Files	D
		Configure InfoPath Forms Services Web Service Proxy	E
Crawler Impact Rules		C	
The Site Directory		D	
Scan Site Directory Links		S	
Farm Search Administration		F	
Custom Properties		P	
Web Application Level			
Send to Connections		C	

Operation and Hot Key			
Document Conversions		D	
SharePoint Designer Settings		S	
Alternate Access Mappings		A	
Custom Properties		P	
Site Collection Level			
Search Settings (hidden when specifying the site collection on the SharePoint 2013 farm)	E	Search Setting	A
		Search Scopes	B
		Search Keywords	C
Quotas and Locks		Q	
Deploy Site Maximum Depth		D	
Visual Upgrade (hidden when specifying the site collection on the SharePoint 2013 farm)		V	
RSS		S	
Help Settings		H	
SharePoint Designer Settings		S	
Custom Properties		P	
Site Level			
RSS Setting		R	
Search and Offline Availability		S	
Related Links Scope Settings (hidden when specifying the site on the SharePoint 2013 farm)		L	
Title, Description, and Icon		I	
Quick Launch		Q	
Top Link Bar		B	
Tree View		V	
Site Theme ("Change the Look" when specifying the site on the SharePoint 2013 farm)		M	
Custom Properties		C	
List/Library Level			
Versioning Settings		E	
Advanced Settings		A	
Validation Settings		V	
General Settings	G	Column Default Value Settings	A
		Rating Settings	B
		Audience Targeting Settings	C
		Metadata Navigation Settings (hidden when specifying the site on the SharePoint 2013 farm)	D
		Pre-location View Settings (hidden when specifying the site on the SharePoint 2013 farm)	E
		RSS Settings	F
Title, Description and Navigation		N	

Security Tab

Operation and Hot Key			
Farm Level			
Security Search	S	Security Search Wizard Mode	A
		Security Search Form Mode	B
		Start with a Predefined Search	C
General Security	G	Configure Managed Accounts	A
		Configure Service Accounts	B
		Configure Password Changes Settings	C
		Manage Trust	E
		Manage Antivirus Settings	F
		Define Blocked File Types	G
		Manage Web Part Security	H
Clone Permissions	C	Clone User Permissions	U
		Clone Site Permissions	S
Import Configuration File		I	
Configure Information Rights Management		M	
Configure Information Management Policy		P	
Dead Account Cleaner	D	Plan Mode	P
		Scan Mode	S
Job Monitor		J	
Web Application Level			
Authentication Providers		V	
Self-Service Site Creation		F	
Security Search	S	Security Search Wizard Mode	A
		Security Search Form Mode	B
		Start with a Predefined Search	C
Blocked File Types		B	
User Permissions		M	
Web Part Security		W	
Clone Permissions	C	Clone User Permissions	U
		Clone Site Permissions	S
User Policy		U	
Anonymous Policy		A	
Permission Policy		P	
Dead Account Cleaner	D	Plan Mode	P
		Scan Mode	S
Job Monitor		J	
Site Collection Level			
Users and Permissions	U	People and Groups	P
		Site Permissions	S
Security Search	S	Security Search Wizard Mode	A
		Security Search Form Mode	B
		Start with a Predefined Search	C
Clone Permissions	C	Clone User Permissions	U

Operation and Hot Key			
		Clone Site Permissions	S
Grant Permissions		G	
Create Group		N	
Export Groups for Editing		R	
Delete Users and Groups		X	
Edit User Permissions		E	
Stop Inheriting Permissions	T	Break Inheritance for Selected Node	A
		Break Inheritance for Sub-nodes	S
Site Collection Administrators	M	Site Collection Administrators	A
		Primary and Secondary Administrators	P
Anonymous Access		A	
Permission Levels		P	
Dead Account Cleaner	D	Plan Mode	P
		Scan Mode	S
Job Monitor		J	
Site Level			
Users and Permissions	U	People and Groups	P
		Site Permissions	S
Security Search	S	Security Search Wizard Mode	A
		Security Search Form Mode	B
		Start with a Predefined Search	C
Clone Permissions	C	Clone User Permissions	U
		Clone Site Permissions	S
Grant Permissions		G	
Create Group		N	
Stop Inheriting Permissions	T	Break Inheritance for Selected Node	A
		Break Inheritance for Sub-nodes	S
Inherit Permissions		I	
Anonymous Access		A	
Permission Levels		P	
Edit User Permissions		E	
Alert Me	M	User Alerts	U
		Search Alerts	S
Dead Account Cleaner	D	Plan Mode	P
		Scan Mode	S
Job Monitor		J	
List/Library Level			
List/Library Permissions		L	
Security Search	S	Security Search Wizard Mode	A
		Security Search Form Mode	B
		Start with a Predefined Search	C
Clone Permissions	C	Clone User Permissions	U
		Clone List/Library Permissions	L
Grant Permissions		G	

Operation and Hot Key			
Anonymous Access	A		
Stop Inheriting Permissions	T	Break Inheritance for Selected Node	A
		Break Inheritance for Sub-nodes	S
Inherit Permissions	I	Apply Inheritance to Selected Node	A
		Push Inheritance to Sub-nodes	S
Alert Me	M	Set alert on this library/list	L
		Manage My Alerts	M
Job Monitor	J		
Folder Level			
Folder Permissions	P		
Security Search	S	Security Search Wizard Mode	A
		Security Search Form Mode	B
		Start with a Predefined Search	C
Clone Permissions	C	Clone User Permissions	U
		Clone Folder Permissions	F
Grant Permissions	G		
Stop Inheriting Permissions	T	Break Inheritance for Selected Node	A
		Break Inheritance for Sub-nodes	S
Inherit Permissions	I	Apply Inheritance to Selected Node	A
		Push Inheritance to Sub-nodes	S
Alert Me	M		
Job Monitor	J		
Item Level			
Item Permissions	P		
Security Search	S	Security Search Wizard Mode	A
		Security Search Form Mode	B
		Start with a Predefined Search	C
Grant Permissions	G		
Stop Inheriting Permissions	T	Break Inheritance for Selected Node	A
		Break Inheritance for Sub-nodes	S
Inherit Permissions	I	Apply Inheritance to Selected Node	A
		Push Inheritance to Sub-nodes	S
Alert Me	M		
Job Monitor	J		

Security Search Wizard Mode

Operation		Hot Key	
Back		B	
Next		N	
Finish	F	Finish and Run Now	R
		Finish	F
Cancel		C	

Break Inheritance for Sub-nodes/Push Inheritance to Sub-nodes

Operation		Hot Key	
OK	S	OK and Run Now	R
		OK	S
Cancel		C	

Permission Tools

Operation		Hot Key	
Stop Inheriting Permissions	T	Break Inheritance for Selected Node	A
		Break Inheritance for Sub-nodes	S
Close		X	

Search Result Tools Tab for Security Search

Operation	Hot Key
Add Users	A
Edit Group Permissions	P
Site Collection Administrators	M
Clone User Permissions	U
Dead Account Cleaner	C
Download Report	L
Export for Editing	E
Import Configuration File	I
Close	X

Policy Enforcer Tab

Operation	Hot Key
Create or Apply Profile	CA
Profile Manager	PM
Generate Report	G
Source Management	S
Filter Policy	F
Policy Enforcer Database	PE
Job Monitor	J

Create or Apply Profile

Operation		Hot Key	
Add Rule	AR	OK	O
		Cancel	C
Remove Rule		RR	

Operation		Hot Key	
Configure Rule	CR	OK	O
		Cancel	C
Activate		AC	
Deactivate		DE	
Profile Manager		PM	
Inherit		I	
Stop Inheriting		S	
Remove Profile		RP	
Job Monitor		J	
Apply	F	Apply	AP
		Apply and Run Now	AR
Run Now		RN	
Cancel		C	

Profile Manager

Operation		Hot Key			
Create Profile	CP	Add Rule	AR		
		Remove Rule	RR		
		Configure Rule	CR		
		Activate	AC		
		Deactivate	DE		
		Save	S	Save	S
				Save and Run Now	R
		Close	X		
View Details	V	Edit	E		
		Close	X		
Edit		E			
Delete		D			
Profile Scope	PS	Remove Profile	RP		
		Close	X		
		Cancel	C		
Run Now		RN			
Job Monitor		J			
Close		X			

Source Collection Policy

Operation		Hot Key	
Create		C	
Set as Default		SD	
Edit	E	Configure	F
		Enable	E
		Disable	D
		Save	S
		Cancel	C
Delete		D	
Close		X	

Policy Enforcer Database

Operation	Hot Key
OK	O
Cancel	C

Generate Report

Operation		Hot Key	
Fix		F	
Manual Operation Required		M	
Hide	H	Hide for a Day	D
		Hide for a Week	W
		Hide for a Month	M
Hidden List	L	Change Expiration Date	C
		Unhide	U
		Close	X
Export	E	OK	O
		Cancel	C
Close		X	

Plan Manager Tab

Operation	Hot Key
View Details	V
Edit	E
Delete	D
Run Now	R
Job Monitor	J

View Details

Operation	Hot Key

Operation	Hot Key
Edit	E
Close	X

Edit

Operation		Hot Key	
Save	S	Save and Run Now	R
		Save	S
Cancel		C	

DocAve Administrator for SharePoint Use Cases

The following use cases apply the procedures described in this guide to several real-world situations. These use cases are intended to give the user an idea of when and why one would use common DocAve Administrator functionality.

Security Permissions Search

Joe was just hired as the head of the IT department for a medium-sized company in New York City. Joe learned that all of the company's relevant electronic documentation was recently imported into Microsoft SharePoint. This information includes employee data (such as addresses and contact information), company accounting records, and Human Resources (HR) documents related to employee salaries.

As his first order of business, Joe is tasked by the company Vice President with reviewing and updating permissions for users and groups who access the HR site collection and the Accounting site collection. Joe wants to maintain what are known as "ethical walls": ensuring that HR sites are accessible to only the appropriate HR groups, Accounting sites are accessible only to the appropriate Accounting groups, etc. In addition, Joe wants to export reports of the user/group permissions, by site collection, and submit them to company the Vice President.

First, Joe performs a security search (Performing a Security Search using Security Search Wizard) on the HR site collection. (He chose using the Wizard over form mode because he is a new user and unfamiliar with the security search options. Joe does not specify a user or group in the search criteria; he wants to review all of the users and their permissions for the selected Site Collection. Upon completion of the security search, Joe reviews the users and permission settings; he ensures that only HR members and HR groups have appropriate permissions to the sites within the HR site collection. Joe notices that the Accounting group has View Only access to a certain subsite within the HR site collection, which is not acceptable. So Joe removes the Accounting group from the HR site collection permissions list. Joe then performs these same actions for the Accounting site collection, verifying the appropriate users/groups and permissions for those sites. All of these actions are done from the security search results panel in Job Monitor.

Now that he has confirmed appropriate user permissions to the site collections in question, Joe wants to generate and submit a report. Joe performs a security search (Performing a Security Search using Security Search Form Mode) on the HR site collection, accesses Job Monitor when the search completes, and downloads the security search report (Downloading Security Search Reports) on the search results. Joe performs these same actions for the Accounting site collection. Joe submits the electronic files to the Vice President for verification.

Employee Shuffling and Permissions Cloning

After verifying the permissions settings for the HR and Accounting site collections (as described in the previous section), Joe is faced with a new task. A Product Manager (PM) named Bettie is being promoted to Vice President of Sales, as the old VP of Sales is retiring. As a result of her promotion, a Sales Representative (SR) named John is being promoted to PM in order to fill the vacant PM position. To perform their job functions, Bettie and John were assigned assorted permission levels on a number of different sites within different site collections, as well as permissions to various libraries and lists. Each of their username's permissions were numerous and unique. Further, a new SR named George was hired. Joe is instructed to quickly update the permissions of Bettie, John, and George so that all three have permissions appropriate to their positions.

Rather than update each user with various permissions for each site, library, and list (which would be a very time-consuming task), Joe knows that with DocAve Administrator, he can quickly complete this assignment. Joe accesses the Cloning User Permissions feature.

1. Joe enters John's username into the **Clone User Permissions from** field, and adds George's username to the **Clone User Permissions to** field. He selects to **Append** John's permissions to George's permissions; George does not yet have permissions assigned to his username. Joe performs the permission transfer.

2. Joe accesses **Clone User Permissions** and enters Bettie's username into the **Clone User Permissions from** field, and adds John to the **Clone User Permissions to** field. He selects to **Replace** John's permissions with Bettie's permissions and performs the permission transfer.

3. Joe again accesses **Clone User Permissions** and enters the outgoing VP's username into the **Clone User Permissions from** field, and adds Bettie to the **Clone User Permissions to** field. He selects to **Replace** Bettie's permissions with the old VP's permissions and performs the permission transfer.

With these three steps, Joe has successfully applied the appropriate permissions to these three users. However, one more step remains. Joe prefers to remove dead accounts from the SharePoint environment. For this task, Joe uses DocAve Administrator's Dead Account Cleaner (Using Dead Account Cleaner). He performs a search of the farm, locates the outgoing VP's account, and deletes the VP's username.

Solution to a Database Becoming Too Large

As a company grows, the data in SharePoint SQL Servers grows as well. As head of the IT department for his employer, Joe is responsible for the managing these SQL databases. One of this primary concerns is enforcing Microsoft's best practices as it relates to SQL Server data storage. Microsoft recommends that SharePoint 2010 content databases not exceed 200 GB of collaborative content. Joe notices that one of his company's content databases is nearing that limit.

Joe's solution to this issue is to first create a site collection ([Creating Site Collections and Content Databases)](). From the **Management** tab, Joe selects **New** > **New Content Database**. He configures the database appropriately, and adds it to the applicable farm.

Next, Joe wants to move the site collection ([Moving Site Collections across Content Databases]()) from the nearly-full content database to the content database he just created. Joe selects the site collection from the **Scope** panel and clicks **Move** from the **Management** tab. Joe selects **Move to Another Database** and selects the destination content database. In this case, he selects the database he just created as the destination content database. Joe clicks **OK** and initiates the action. The site collections are moved across databases.

Joe now wants to run the broken link checker ([Checking for Broken Links)]() to ensure that all links across site collections are still intact. He searches for broken links across both content databases and discovers no broken links. Lastly, Joe runs the orphan site deletion ([Deleting Orphan Sites)]() search to see if any orphan sites were created during the site collection migration. He runs a separate search of each content database, and discovers that there are no orphan sites.

Appendix A: Search Filter Table

Search Filter Table for Most Filter Conditions

The table below contains the detailed information of all the filter conditions except **User and Group**.

Level	Rule	Condition		Value	Result
Web Application	URL	Contains		tes	The Web application whose URL contains **tes** is searched. Search result example: **http://tes:30000/** and **http://test:20000/**
		Equals		http://test:20000/	The Web application whose URL is **http://test:20000/** is searched.
		Matches		http://tes*000/	The Web application whose URL begins with **http://tes** and ends with **000/** is searched. Search result example: **http://test:20000/**
				http://te?t:2000?/	The Web application whose URL is the same as **http://te?t:20000/** except character **?**. Search result example: **http://test:20001/** and **http://text:20002/**
	Custom Property: Text	Manually input the property name. Using this condition if you want to search Web applications according to their custom property values. This condition	Contains	intranet	The Web application that has the specified custom property and the property value contains **intranet** is searched.
			Does Not Contain	intranet	The Web application that has the specified custom property and the property value contains **intranet** is searched.
			Equals	intranet	The Web application that has the specified custom property and the property value is equal to **intranet** is searched.
			Does Not Equal	intranet	The Web application that has the specified custom property and the property value is not equal to **intranet** is searched.

Level	Rule	Condition		Value	Result
		supports all the custom property types except Number, Yes/No, Data and Time types. You can check existing custom properties or add new properties from **Configuration** tab > **Custom Property**.	Matches	intranet*com	The Web application that has the specified custom property and the property value starts with **intranet** and ends with **com** is searched. The Match filter rule supports wildcard (*).
				intranet?co?	The Web application that has the specified custom property and the property value is the same as **intranet?co?** except character **?**. The character **?** represents any character.
			Does Not Match	intranet*com	The Web application that has the specified custom property and the property value neither begins with **intranet** nor ends with **com** is searched.
				Intranet?co?	The Web application that has the specified custom property and the property value is not **intranet?co?** is searched. The character? represents any character.
	Custom Property: Number	Manually input the property name. This condition only supports Number property type.	>=	10	The Web application that has the specified custom property and the property value is larger than or equal to **10** is searched.
			<=	10	The Web application that has the specified custom property and the property value is smaller than or equal to **10** is searched.
			=	10	The Web application that has the specified custom property and the property value is equal to **10** is searched.
	Custom Property: Yes/No	Manually input the property name. This condition only supports Yes/No property type.	Equals	Yes	The Web application that has the specified custom property and the property value is **Yes** is searched.
				No	The Web application that has the specified custom property and the property value is **No** is searched.

Level	Rule	Condition	Value	Result
	Custom Property: Data/Time	Manually input the property name. This condition only supports Data and Time property type.	From…To	2011-11-11 12:15:50 2011-12-25 17:35:54	The Web application that has the specified custom property and the property value is **12:15:50 11/11/2011** to **17:35:54 12/25/2011** is searched.
			Before	2011-11-11 12:15:50	The Web application that has the specified custom property and the property value is before **12:15:50 11/11/2011** is searched.
			After	2011-11-11 12:15:50	The Web application that has the specified custom property and the property value is after **12:15:50 11/11/2011** is searched.
			On	2011-11-11	The Web application that has the specified custom property and the property value is **11/11/2011** is searched.
			Within days/weeks/months/years	5 **Days**	The Web application that has the specified custom property and the property value is in last **5** days is searched.
			Older Than[Years/Months/Weeks/Days]	5 **Days**	The Web application that has the specified custom property and the property value is older than **5** days is searched.
Site Collection	URL	Contains		sitecollection	The site collection whose URL contains **sitecollection** is searched. Search result example: **http://test:20000/sites/ sitecollectionA** and **http://test:20000/sites/ sitecollectionB**
		Equals		http://test:20000/ sites/sitecollection A	The site collection whose URL is **http://test:20000/sites/ sitecollectionA** is searched.
		Matches		http://tes*collec-tionA	The site collection whose URL begins with **http://tes** and ends with **collectionA** is searched. Search result example: **http://tesABC:11111/ sitecollectionA**

Level	Rule	Condition	Value	Result
			http://test:20000/ sites/sitecollecti?n A	The site collection whose URL is the same as **http://test:20000/sites/ sitecollecti?nA** except character **?** is searched. Search result example: **http://test:20000/sites/ sitecollectionA** and **http://text:20000/sites/ sitecollectiBnA**
	Site Collection Title	Contains	title	The site collection whose title contains **title** is searched. Search result example: **titleA** and **title1**
		Equals	title1	The site collection whose tile is **title1** is searched.
		Matches	ti*1	The site collection whose title begins with **ti** and ends with **1** is searched. Search result example: **title1**
			tit?e1	The site collection whose title is the same as **tit?e1** except character **?** is searched. The character **?** represents any character. Search result example: **titAe1** and **titBe1**.
	Modified Time	From…To	2011-11-11 12:15:50 2011-12-25 17:35:54	The site collection that is modified between **12:15:50 11/11/2011** and **17:35:54 12/25/2011** is searched.
		Before	2011-11-11 12:15:50	The site collection that is modified before **12:15:50 11/11/2011** is searched.
		After	2011-11-11 12:15:50	The site collection that is modified after **12:15:50 11/11/2011** is searched.
		On	2011-11-11	The site collection that is modified on **11/11/2011** is searched.
		Within days/weeks/months/ years	5 **Days**	The site collection that is modified in last **5** days is searched.

Level	Rule	Condition	Value	Result
	Created Time	From…To	2011-11-11 12:15:50 2011-12-25 17:35:54	The site collection that is created between **12:15:50 11/11/2011** and **17:35:54 12/25/2011** is searched.
		Before	2011-11-11 12:15:50	The site collection that is created before **12:15:50 11/11/2011** is searched.
		After	2011-11-11 12:15:50	The site collection that is created after **12:15:50 11/11/2011** is searched.
		On	2011-11-11	The site collection that is created on **11/11/2011** is searched.
		Within days/weeks/months/ years	5 **Days**	The site collection that is created in last **5** days is searched.
	Primary Admin-istrator	Contains	user	The site collection whose primary administrator's name contains **user** is searched. Search result example: **userA** and **user1**
		Equals	userA	The site collection whose primary administrator's name is **userA** is searched.
	Template Name	Contains	Team	The site collection whose template name contains **Team** is searched. Search result example: **Team Site**
		Equals	Blank Site	The site collection whose template name is **Blank Site** is searched.
		Matches	B*Workspace	The site collection whose template name begins with **B** and ends with **Workspace** is searched. Search result example: **Basic Meeting Workspace** and **Blank Meeting Workspace**
			Bl?g	The site collection whose template name is the same as **Bl?g** except character **?** is searched. Search result example: **Blog** and **Bldg**
	Auditing	Equals	Enabled	The site collection with Auditing enabled is searched.

Level	Rule	Condition		Value	Result
				Disabled	The site collection with Auditing disabled is searched.
	Anonymous Access	Equals		Enabled	The site collection with Anonymous Access enabled is searched.
				Disabled	The site collection with Anonymous Access disabled is searched.
	Lock Status	Equals		Not Locked	The site collection whose lock status is Not Locked is searched.
				Adding Content Prevented	The site collection whose lock status is Adding Content Prevented is searched.
				Read Only	The site collection whose lock status is Read Only is searched.
				No Access	The site collection whose lock status is No Access is searched.
	Size	>= MB/GB		10MB	The site collection whose size is larger than or equal to 10MB is searched.
		<= MB/GB		10MB	The site collection whose size is smaller than or equal to 10MB is searched.
		= MB/GB		10MB	The site collection whose size is equal to 10MB is searched.
	Custom Property: Text	Manually input the property name. Using this condition if you want to search site collections according to their custom property values.	Contains	intranet	The site collection that has the specified custom property and the property value contains **intranet** is searched.
			Does Not Contain	intranet	The site collection that has the specified custom property and the property value contains **intranet** is searched.
			Equals	intranet	The site collection that has the specified custom property and the property value is equal to **intranet** is searched.
			Does Not Equal	intranet	The site collection that has the specified custom property and the property value is not equal to **intranet** is searched.

Level	Rule	Condition		Value	Result
		This condition supports all the custom property types except Number, Yes/No, Data and Time types. You can check existing custom properties or add new properties from **Configuration** tab > **Custom Property**	Matches	intranet*com	The site collection that has the specified custom property and the property value starts with **intranet** and ends with **com** is searched. The Match filter rule supports wildcard (*).
				intranet?com	The site collection that has the specified custom property and the property value is the same as **intranet?com** except character **?**. The character **?** represents any character.
			Does Not Match	intranet*com	The site collection that has the specified custom property and the property value begins with **intranet** and ends with **com** is not searched.
				intranet?com	The site collection that has the specified custom property and the property value is not **intranet?com** is searched. The character? represents any character.
	Custom Property: Number	Manually input the property name. This condition only supports Number property type.	>=	10	The site collection that has the specified custom property and the property value is larger than or equal to **10** is searched.
			<=	10	The site collection that has the specified custom property and the property value is smaller than or equal to **10** is searched.
			=	10	The site collection that has the specified custom property and the property value is equal to **10** is searched.
	Custom Property: Yes/No	Manually input the property name.	Equals	Yes	The site collection that has the specified custom property and the property value is **Yes** is searched.

Level	Rule	Condition		Value	Result
		This condition only supports Yes/No property type.		No	The site collection that has the specified custom property and the property value is **No** is searched.
	Custom Property: Data/Time	Manually input the property name. This condition only supports Data and Time property type.	From…To	2011-11-11 12:15:50 2011-12-25 17:35:54	The site collection that has the specified custom property and the property value is **12:15:50 11/11/2011** to **17:35:54 12/25/2011** is searched.
			Before	2011-11-11 12:15:50	The site collection that has the specified custom property and the property value is before **12:15:50 11/11/2011** is searched.
			After	2011-11-11 12:15:50	The site collection that has the specified custom property and the property value is after **12:15:50 11/11/2011** is searched.
			On	2011-11-11	The site collection that has the specified custom property and the property value is **11/11/2011** is searched.
			Within days/weeks/months/years	5 Days	The site collection that has the specified custom property and the property value is in last **5** days is searched.
			Older Than[Years/Months/Weeks/Days]	5 Days	The site collection that has the specified custom property and the property value is older than **5** days is searched.
Site	URL	Contains		siteA	The site whose URL contains **siteA** is searched. Search result example: **http://test:20000/sites/site-collectionA/siteA** and **http://test:20000/sites/site-collectionA/siteAB**
		Equals		http://test:20000/sites/sitecollectionA/siteA	The site whose URL is **http://test:20000/sites/sitecollectionA/siteA** is searched.

Level	Rule	Condition	Value	Result
		Matches	http://tes*siteA	The site whose URL begins with **http://tes** and ends with **siteA** is searched. Search results example: **http://tesABC:11111/site-collectionA/siteA**
			http://test:20000/ sites/sitecollection ?/siteA	The site whose URL is the same as **http://test:20000/sites/site-collection?/siteA** except character **?** is searched. Search result example: **http://test:20000/sites/site-collectionA/siteA**
	Site Title	Contains	title	The site whose title contains **title** is searched. Search result example: **titleA** and **title1**
		Equals	title1	The site collection whose title is **title1** is searched.
		Matches	ti*1	The site whose title begins with **ti** and ends with **1** is searched. Search result example: **title1**
			tit?e1	The site whose title is the same as **tit?e1** except character **?** is searched. Search result example: **titAe1**
	Modified Time	From…To	2011-11-11 12:15:50 2011-12-25 17:35:54	The site that is modified between **12:15:50 11/11/2011** and **17:35:54 12/25/2011** is searched.
		Before	2011-11-11 12:15:50	The site that is modified before **12:15:50 11/11/2011** is searched.
		After	2011-11-11 12:15:50	The site that is modified after **12:15:50 11/11/2011** is searched.
		On	2011-11-11	The site that is modified on **11/11/2011** is searched.
		Within days/weeks/months/ years	5 Days	The site that is modified in last **5** days is searched.
	Created Time	From…To	2011-11-11 12:15:50 2011-12-25 17:35:54	The site that is created between **12:15:50 11/11/2011** and **17:35:54 12/25/2011** is searched.

Level	Rule	Condition	Value	Result
		Before	2011-11-11 12:15:50	The site that is created before **12:15:50 11/11/2011** is searched.
		After	2011-11-11 12:15:50	The site that is created after **12:15:50 11/11/2011** is searched.
		On	2011-11-11	The site that is created on **11/11/2011** is searched.
		Within days/weeks/months/ years	5 **Days**	The site that is created in last **5** days is searched.
	Created By	Contains	user	The site created by the user whose name contains **user** is searched. Search result example: **userA** and **user1**
		Equals	userA	The site created by the user whose name is **userA** is searched.
	Template Name	Contains	Team	The site whose template name contains **Team** is searched. Search result example: **Team Site**
		Equals	Blank Site	The site whose template name is **Blank Site** is searched.
		Matches	B*Workspace	The site whose template name begins with **B** and ends with **Workspace** is searched. Search result example: **Basic Meeting Workspace** and **Blank Meeting Workspace**
			Bl?g	The site whose template name is the same as **Bl?g** except character **?** is searched. Search result example: **Blog**
	Anonymous Access	Equals	Enabled	The site with Anonymous Access enabled is searched.
			Disabled	The site with Anonymous Access disabled is searched.
	Inheritance	Equals	Inherited Permission	The site that has inherited permission from its parent node is searched.

Level	Rule	Condition		Value	Result
				Explicit Permissions	The site that has explicit permission is searched.
	Auditing	Equals		Enabled	The site with Auditing enabled is searched.
				Disabled	The site with Auditing disabled is searched.
	Custom Property: Text	Manually input the property name. Using this condition if you want to search sites according to their custom property values. This condition supports all the custom property types except Number, Yes/No, Data and Time types. You can check existing custom properties or add new properties from **Configuration**	Contains	intranet	The site that has the specified custom property and the property value contains **intranet** is searched.
			Does Not Contain	intranet	The site that has the specified custom property and the property value contains **intranet** is searched.
			Equals	intranet	The site that has the specified custom property and the property value is equal to **intranet** is searched.
			Does Not Equal	intranet	The site that has the specified custom property and the property value is not equal to **intranet** is searched.
			Matches	intranet*com	The site that has the specified custom property and the property value starts with **intranet** and ends with **com** is searched. The Match filter rule supports wildcard (*).
				intranet?com	The site that has the specified custom property and the property value is the same as **intranet?com** except character **?**. The character **?** represents any characters.
			Does Not Match	intranet*com	The site that has the specified custom property and the property value begins with **intranet** and ends with **com** is not searched.

Level	Rule	Condition		Value	Result
		tab > **Custom Property**.		intranet?com	The site that has the specified custom property and the property value is not **intranet?com** is searched. The character? represents any character.
	Custom Property: Number	Manually input the column name. This condition only supports Number column type.	>=	10	The site that has the specified custom property and the property value is larger than or equal to **10** is searched.
			<=	10	The site that has the specified custom property and the property value is smaller than or equal to **10** is searched.
			=	10	The site that has the specified custom property and the property value is equal to **10** is searched.
	Custom Property: Yes/No	Manually input the column name. This condition only supports Yes/No column type.	Equals	Yes	The site that has the specified custom property and the property value is **Yes** is searched.
				No	The site that has the specified custom property and the property value is **No** is searched.
	Custom Property: Data/Time	Manually input the column name. This condition only supports Data and Time column type.	From...To	2011-11-11 12:15:50 2011-12-25 17:35:54	The site that has the specified custom property and the property value is **12:15:50 11/11/2011** to **17:35:54 12/25/2011** is searched.
			Before	2011-11-11 12:15:50	The site that has the specified custom property and the property value is before **12:15:50 11/11/2011** is searched.
			After	2011-11-11 12:15:50	The site that has the specified custom property and the property value is after **12:15:50 11/11/2011** is searched.
			On	2011-11-11	The site that has the specified custom property and the property value is **11/11/2011** is searched.

Level	Rule	Condition		Value	Result
			Within days/weeks/months/years	5 **Days**	The site that has the specified custom property and the property value is in last **5** days is searched.
			Older Than	5 **Days**	The site that has the specified custom property and the property value is older than **5** days is searched.
List/Library	URL	Contains		libraryA	The library whose URL contains **libraryA** is searched. Search result example: **http://test:20000/sites/sitecollectionA/siteA/LibraryA** and **http://test:20000/sites/stiecollectionA/siteA/libraryAB**
		Equals		http://test:20000/sites/sitecollectionA/siteA/LibraryA	The library whose URL is **http://test:20000/sites/site-collectionA/siteA/libraryA**
		Matches		http://test:20000/*/LibraryA	The library whose URL begins with **http://test:20000/** and ends with **LibraryA** is searched. Search result example: **http://test:20000/sites/sitecollectionA/siteA/LibraryA** and **http://test:20000/sites/sitecollectionB/siteB/LibraryA**
				http://te?t:20000/sites/sitecollectionA/siteA/LibraryA	The library whose URL is the same as http://te?t:20000/sites/sitecollectionA/siteA/LibraryA except character**?** is searched. Search result example: **http://test:20000/sites/sitecollectionA/siteA/LibraryA** and **http://text:20000/sites/sitecollectionA/siteA/LibraryA**.
	Name	Contains		lib	The library whose name contains **lib** will be searched out. For example, **libraryA** and **lib123** is searched.

Level	Rule	Condition	Value	Result
		Equals	libraryA	The library whose name is **libraryA** is searched.
		Matches	li*A	The library whose title begins with **li** and ends with **A** is searched. Search result example: **libraryA**
			libra?yA	The library whose title is the same as **librara?yA** except character **?** is searched. Search results example: **libraryA**
	Modified Time	From…To	2011-11-11 12:15:50 2011-12-25 17:35:54	The list/library that is modified between **12:15:50 11/11/2011** and **17:35:54 12/25/2011** is searched.
		Before	2011-11-11 12:15:50	The list/library that is modified before **12:15:50 11/11/2011** is searched.
		After	2011-11-11 12:15:50	The list/library that is modified after **12:15:50 11/11/2011** is searched.
		On	2011-11-11	The list/library that is modified on **11/11/2011** is searched.
		Within days/weeks /months/ years	5 **Days**	The list/library that is modified in last **5** days is searched.
	Created Time	From…To	2011-11-11 12:15:50 2011-12-25 17:35:54	The list/library that is created between **12:15:50 11/11/2011** and **17:35:54 12/25/2011** is searched.
		Before	2011-11-11 12:15:50	The list/library that is created before **12:15:50 11/11/2011** is searched.
		After	2011-11-11 12:15:50	The list/library that is created after **12:15:50 11/11/2011** is searched.
		On	2011-11-11	The list/library that is created on **11/11/2011** is searched.
		Within days/weeks/months/ years	5 **Days**	The list/library that is created in last **5** days is searched.

Level	Rule	Condition	Value	Result
	Created By	Contains	use	The list/library created by the user whose name contains **use** is searched. Search result example: **userA**
		Equals	userA	The list/library that is created by **userA** is searched.
	Anonymous Access	Equals	Enabled	The list/library with Anonymous Access enabled is searched.
			Disabled	The list/library with Anonymous Access disabled is searched.
	Inheritance	Equals	Inherited Permission	The list/library that has inherited permission from its parent node is searched.
			Explicit Permissions	The list/library that has explicated permission is searched.
	Auditing	Equals	Enabled	The list/library with Auditing enabled is searched.
			Disabled	The list/library with Auditing disabled is searched.
	Versioning	Equals	Enabled	The list/library with Versioning enabled is searched.
			Disabled	The list/library with Versioning disabled is searched.
Folder	Name	Contains	folder	The folder whose name contains **folder** is searched.
		Equals	folderA	The folder whose name is **folderA** is searched.
		Matches	fol*A	The folder whose name begins with **fol** and ends with **A** is searched.
			fold?rA	The folder whose name is the same as **fold?rA** except character **?** is searched. Search results example: **folderA**
	Inheritance	Equals	Inherited Permission	The folder that has inherited permission from its parent node is searched.

Level	Rule	Condition	Value	Result
			Explicit Permissions	The folder that has explicated permission is searched.
	Auditing	Equals	Enabled	The folder with Auditing enabled is searched.
			Disabled	The folder with Auditing disabled is searched.
Item	Name	Contains	item	The item whose name contains **item** is searched.
		Equals	itemA	The item whose name is **itemA** is searched.
		Matches	it*A	The item whose name begins with **it** and ends with is searched. Search result example: **itemA**
			ite?A	The item whose name is the same as **ite?A** except character **?** is searched. Search result example: **itemA**
	Inheritance	Equals	Inherited Permission	The item that has inherited permission from its parent node is searched.
			Explicit Permissions	The item that has explicated permission is searched.
	Content Type	Equals	typeA	The item whose content type is **typeA** is searched.
	Versions	Only Latest [] Versions	3	The item's last 3 versions are searched.
		Only Latest [] Major Versions	3	The item's last 3 major versions are searched.
		Only Major Versions	N/A	All major versions are searched.
		Only Approved Versions	N/A	All approved versions are searched.
Document	Document Name And Extension	Contains	doc	The document whose document name and extension contains demo is searched.
		Equals	demo.doc	The document whose document name and extension is **demo.doc** is searched.
		Matches	dem*lsc	The document whose document name and extension begins with **dem** and ends with **lsc** is searched.

Level	Rule	Condition	Value	Result
			demo.x?sc	The document whose document name and extension is the same as **demo.x?sc** except character **?** is searched.
	Inheritance	Equals	Inherited Permission	The document that has inherited permission from its parent node is searched.
			Explicit Permissions	The document that has explicated permission is searched.
	Content Type	Equals	typeA	The item whose content type is **typeA** is searched.
	Versions	Only Latest [] Versions	3	The file's last 3 versions are searched.
		Only Latest [] Major Versions	3	The file's last 3 major versions are searched. If a file has the following versions: 1.0, 2.0, 2.1, 2.2, 3.0, 3.1, the search result example is: version 1.0, 2.0, 3.0
		Only Major Versions	N/A	All major versions are searched.
		Only Approved Versions	N/A	All approved versions are searched.

Search Filter Table for User and Group Filter Condition

The table below contains detailed information on the **User and Group** filter condition.

Level	Rule	Condition	Value	Permission	Query Mode	Result
Site Collection ***Note**: For other levels (i.e. Site, List/Library, Folder, Item, Document), the filter rules are similar.	User And Group	Equals	user	Search for any permission	Exact permission	The site collection whose user name is **user** is searched without regard to **user**'s permission.
					Exact permission or better	The site collection whose user name is **user** is searched without regard to **user**'s permission.
			user	Full Control	Exact permission	The site collection whose user name is **user** and whose user permission is **Full Control** is searched.
			user		Exact permission or better	N/A
			user	Design	Exact permission	The site collection whose user name is **user** and whose user permission is **Design** is searched.

Level	Rule	Condition	Value	Permission	Query Mode	Result
			user		Exact permission or better	The site collection whose user name is **user** and whose user permission is equal or better than **Design** is searched.
			user	Edit	Exact permission	The site collection whose user name is **user** and user permission is **Edit** is searched.
			user		Exact permission or better	The site collection whose user name is **user** and user permission is equal or better than **Edit** is searched.
			user	Contribute	Exact permission	The site collection whose user name is **user** and whose user permission is **Contribute** is searched.
			user		Exact permission or better	The site collection whose user name is **user** and whose user permission is equal or better than **Contribute** is searched.
			user	Read	Exact permission	The site collection whose user name is **user** and whose user permission is **Read** is searched.
			user		Exact permission or better	The site collection whose user name is **user** and whose user permission is equal or better than **Read** is searched.
			user	View Only	Exact permission	The site collection whose user name is **user** and whose user permission is **View Only** is searched.
			user		Exact permission or better	The site collection whose user name is **user** and whose user permission is equal or better than **View Only** is searched.
			user	Limited Access	Exact permission	The site collection whose user name is **user** and whose user permission is **Limited Access** is searched.
			user		Exact permission or better	The site collection whose user name is **user** and whose user permission is equal or better than **Limited Access** is searched.

Appendix B: DocAve Administrator and SharePoint Operations

Some DocAve Administrator functions are unique to DocAve, while some also available in SharePoint. Refer to the tables below for more information about all these functions.

Farm Level Operations

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings
Management					
New	Management > Contribute	Management > Contribute	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Admin Search Wizard Mode	Management > Contribute	Management > Contribute	N/A	N/A	Unsupported
Admin Search Form Mode	Management > Contribute	Management > Contribute	N/A	N/A	Unsupported
Start with a Predefined Search	Management > Contribute	Management > Contribute	N/A	N/A	Unsupported
Manage Farm Features	Management > System Settings	Management > System Settings	Central Administration > System Settings	Central Administration > System Settings	Unsupported
Manage Farm Solutions	Management > System Settings	Management > System Settings	Central Administration > System Settings	Central Administration > System Settings	Unsupported
Manage User Solutions	Management > System Settings	Management > System Settings	Central Administration > System Settings	Central Administration > System Settings	Unsupported
Servers in Farm	Management > System Settings	Management > System Settings	Central Administration > System Settings	Central Administration > System Settings	Unsupported
Services on Server	Management > System Settings	Management > System Settings	Central Administration > System Settings	Central Administration > System Settings	Unsupported
Quiesce Farm	Management > System Settings	Management > System Settings	To achieve by command line.	To achieve by command line.	Unsupported

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings
Manage Service Applications	Management > Application Management	Management > Application Management	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Search Service	Management > Application Management	Unsupported	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Default Database Server	Management > Application Management	Management > Application Management	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Data Retrieval Service	Management > Application Management	Management > Application Management	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Specify Quota Templates	Management > Application Management	Management > Application Management	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Review Database Status	Management > Upgrade and Patch	Management > Upgrade and Patch	Central Administration > Upgrade and Migration	Central Administration > Upgrade and Migration	Unsupported
Check Product and Patch Installation Status	Management > Upgrade and Patch	Management > Upgrade and Patch	Central Administration > Upgrade and Migration	Central Administration > Upgrade and Migration	Unsupported
Search Duplicate Files	Management > Search Gallery	Management > Search Gallery	N/A	N/A	Unsupported
Job Monitor	Management > Statistics	Management > Statistics	N/A	N/A	N/A
Configuration					
Configure Outgoing E-mail Settings	Configuration > Farm Configuration	Configuration > Farm Configuration	Central Administration > System Settings	Central Administration > System Settings	Unsupported
Configure Incoming E-mail Settings	Configuration > Farm Configuration	Configuration > Farm Configuration	Central Administration > System Settings	Central Administration > System Settings	Unsupported
Configure Mobile Account	Configuration > Farm Configuration	Configuration > Farm Configuration	Central Administration > System Settings	Central Administration > System Settings	Unsupported

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings
Alternate Access Mappings	Configuration > Farm Configuration	Configuration > Farm Configuration	Central Administration > System Settings	Central Administration > System Settings	Unsupported
Privacy Options	Configuration > Farm Configuration	Configuration > Farm Configuration	Central Administration > System Settings	Central Administration > System Settings	Unsupported
Cross-Firewall Access Zone	Configuration > Farm Configuration	Configuration > Farm Configuration	Central Administration > System Settings	Central Administration > System Settings	Unsupported
Records Center	Configuration > Farm Configuration	Configuration > Farm Configuration	To achieve by command line.	To achieve by command line.	Unsupported
Manage Form Templates	Configuration > General Application Settings	Configuration > General Application Settings	Central Administration > General Application Settings	Central Administration > General Application Settings	Unsupported
Configure InfoPath Forms Services	Configuration > General Application Settings	Configuration > General Application Settings	Central Administration > General Application Settings	Central Administration > General Application Settings	Unsupported
Upload Form Template	Configuration > General Application Settings	Configuration > General Application Settings	Central Administration > General Application Settings	Central Administration > General Application Settings	Unsupported
Manage Data Connection Files	Configuration > General Application Settings	Configuration > General Application Settings	Central Administration > General Application Settings	Central Administration > General Application Settings	Unsupported
Configure InfoPath Forms Services Web Service Proxy	Configuration > General Application Settings	Configuration > General Application Settings	Central Administration > General Application Settings	Central Administration > General Application Settings	Unsupported
Crawler Impact Rules	Configuration > General Application Settings	Configuration > General Application Settings	Central Administration > General Application Settings	Central Administration > General Application Settings	Unsupported
Scan Site Directory Links	Configuration > General Application Settings	Configuration > General Application Settings	Central Administration > General Application Settings	Central Administration > General Application Settings	Unsupported

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings
The Site Directory	Configuration > General Application Settings	Configuration > General Application Settings	Central Administration > General Application Settings	Central Administration > General Application Settings	Unsupported
Farm Search Administration	Configuration > General Application Settings	Configuration > General Application Settings	Central Administration > General Application Settings	Central Administration > General Application Settings	Unsupported
Custom Properties	Configuration > Customization	Configuration > Customization	N/A	N/A	Unsupported
Security					
Security Search Wizard Mode	Security > Contribute	Security > Contribute	N/A	N/A	Unsupported
Security Search Form Mode	Security > Contribute	Security > Contribute	N/A	N/A	Unsupported
Start with a Predefined Search	Security > Contribute	Security > Contribute	N/A	N/A	Unsupported
Configure Managed Accounts	Security > General Security	Security > General Security	Central Administration > Security	Central Administration > Security	Unsupported
Configure Service Accounts	Security > General Security	Security > General Security	Central Administration > Security	Central Administration > Security	Unsupported
Configure Password Changes Settings	Security > General Security	Security > General Security	Central Administration > Security	Central Administration > Security	Unsupported
Manage Trust	Security > General Security	Security > General Security	Central Administration > Security	Central Administration > Security	Unsupported
Manage Antivirus Settings	Security > General Security	Security > General Security	Central Administration > Security	Central Administration > Security	Unsupported
Define Blocked File Types	Security > General Security	Security > General Security	Central Administration > Security	Central Administration > Security	Unsupported
Manage Web Part Security	Security > General Security	Security > General Security	Central Administration > Security	Central Administration > Security	Unsupported
Clone User Permissions	Security > Permission	Security > Permission	N/A	N/A	Unsupported

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings
Import Configuration File	Security > Permission	Security > Permission	N/A	N/A	Unsupported
Configure Information Rights Management	Security > Information Policy	Security > Information Policy	Central Administration > Security	Central Administration > Security	Unsupported
Configure Information Management Policy	Security > Information Policy	Security > Information Policy	Central Administration > Security	Central Administration > Security	Unsupported
Dead Account Cleaner	Security > Account	Security > Account	N/A	N/A	Unsupported
Search Temporary Permissions	Security > Permission	Security > Permission	N/A	N/A	Supported
Policy Enforcer					
Create or Apply Profile	Policy Enforcer > Policy Enforcer	Policy Enforcer > Policy Enforcer	N/A	N/A	Supported
Profile Manager	Policy Enforcer > Policy Enforcer	Policy Enforcer > Policy Enforcer	N/A	N/A	Unsupported
Generate Report	Policy Enforcer > Report	Policy Enforcer > Report	N/A	N/A	Supported
Source Management	Policy Enforcer > Settings	Policy Enforcer > Settings	N/A	N/A	Unsupported
Policy Enforcer Database	Policy Enforcer > Settings	Policy Enforcer > Settings	N/A	N/A	Unsupported
Filter Policy	Policy Enforcer > Settings	Policy Enforcer > Settings	N/A	N/A	Unsupported

Web Application Level Operations

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings
Management					
New Site Collection	Management > Contribute	Management > Contribute	Central Administration > Application Management	Central Administration > Application	Supported

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings
				Management	
New Content Database	Management > Contribute	Management > Contribute	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Extend	Management > Contribute	Management > Contribute	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Delete Web Application	Management > Contribute	Management > Contribute	Central Administration > Application Management	Central Administration > Application Management	Supported
Remove SharePoint from IIS Web Site	Management > Contribute	Management > Contribute	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Admin Search Wizard Mode	Management > Contribute	Management > Contribute	N/A	N/A	Supported
Admin Search Form Mode	Management > Contribute	Management > Contribute	N/A	N/A	Supported
Start with a Predefined Search	Management > Contribute	Management > Contribute	N/A	N/A	Supported
General Settings	Management > Manage	Management > Manage	Central Administration > Application Management	Central Administration > Application Management	Supported
Resource Throttling	Management > Manage	Management > Manage	Central Administration > Application Management	Central Administration > Application Management	Supported
Workflow	Management > Manage	Management >	Central Administration >	Central	Supported

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings
		Manage	Application Management	Administration > Application Management	
Outgoing Email	Management > Manage	Management > Manage	Central Administration > Application Management	Central Administration > Application Management	Supported
Mobile Account	Management > Manage	Management > Manage	Central Administration > Application Management	Central Administration > Application Management	Supported
Site Use and Deletions	Management > Manage	Management > Manage	Central Administration > Application Management	Central Administration > Application Management	Supported
Manage Features	Management > Manage	Management > Manage	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Manage Paths	Management > Manage	Management > Manage	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Service Connections	Management > Manage	Management > Manage	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Manage Content Databases	Management > Manage Content Databases	Management > Manage Content Databases	Central Administration > Application Management	Central Administration > Application Management	Unsupported

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings
Site Collection List	Management > Manage Content Databases	Management > Manage Content Databases	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Delete Orphan Sites	Management > Manage Content Databases	Management > Manage Content Databases	N/A	N/A	Supported
Search Web Parts	Management > Search Gallery	Management > Search Gallery	N/A	N/A	Supported
Search Duplicate Files	Management > Search Gallery	Management > Search Gallery	N/A	N/A	Supported
Job Monitor	Management > Statistics	Management > Statistics	N/A	N/A	N/A
Configuration					
Send to Connections	Configuration > External Service Connections	Configuration > External Service Connections	Central Administration > General Application Settings	Central Administration > General Application Settings	Unsupported
Document Conversions	Configuration > External Service Connections	Configuration > External Service Connections	Central Administration > General Application Settings	Central Administration > General Application Settings	Unsupported
SharePoint Designer Settings	Configuration > SharePoint Designer	Configuration > SharePoint Designer	Central Administration > General Application Settings	Central Administration > General Application Settings	Unsupported
Alternate Access Mappings	Configuration > Web Application	Configuration > Web Application	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Custom Properties	Configuration > Customization	Configuration > Customization	N/A	N/A	Supported

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings
Security					
Authentication Providers	Security > General Settings	Security > General Settings	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Self-Service Site Creation	Security > General Settings	Security > General Settings	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Security Search Wizard Mode	Security > General Settings	Security > General Settings	N/A	N/A	Supported
Security Search Form Mode	Security > General Settings	Security > General Settings	N/A	N/A	Supported
Start with a Predefined Search	Security > General Settings	Security > General Settings	N/A	N/A	Supported
Blocked File Types	Security > General Settings	Security > General Settings	Central Administration > Application Management	Central Administration > Application Management	Unsupported
User Permissions	Security > General Settings	Security > General Settings	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Web Part Security	Security > General Settings	Security > General Settings	Central Administration > Application Management	Central Administration > Application Management	Supported
Clone User Permissions	Security > Permission	Security > Permission	N/A	N/A	Supported
User Policy	Security > Policy	Security > Policy	Central Administration > Application Management	Central Administration > Application	Unsupported

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings
				Management	
Anonymous Policy	Security > Policy	Security > Policy	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Permission Policy	Security > Policy	Security > Policy	Central Administration > Application Management	Central Administration > Application Management	Unsupported
Dead Account Cleaner	Security > Account	Security > Account	N/A	N/A	Supported
Search Temporary Permission	Security > Permission	Security > Permission	N/A	N/A	Supported
Policy Enforcer					
Create or Apply Profile	Policy Enforcer > Policy Enforcer	Policy Enforcer > Policy Enforcer	N/A	N/A	Supported
Profile Manager	Policy Enforcer > Policy Enforcer	Policy Enforcer > Policy Enforcer	N/A	N/A	Unsupported
Generate Report	Policy Enforcer > Report	Policy Enforcer > Report	N/A	N/A	Supported
Source Management	Policy Enforcer > Settings	Policy Enforcer > Settings	N/A	N/A	Unsupported
Policy Enforcer Database	Policy Enforcer > Settings	Policy Enforcer > Settings	N/A	N/A	Unsupported

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings
Filter Policy	Policy Enforcer > Settings	Policy Enforcer > Settings	N/A	N/A	Unsupported

Site Collection Level Operations

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Management						
New	Management > Contribute	Management > Contribute	Login Site Collection > Site Actions > New Site	Login Site Collection > Site Contents > new subsite	Supported	Create Sub-Sites: Full Control Create List/Lib: Unsupported Create Folder/Item: Contribute
Move	Management > Contribute	Management > Contribute	N/A	N/A	Supported	Unsupported
Delete	Management > Contribute	Management > Contribute	Central Administration > Application Management	Central Administration > Application Management	Supported	Web: Full Control List/Lib: Design Folder/Item: Contribute (Browse: Design)
Admin Search Wizard Mode	Management > Contribute	Management > Contribute	N/A	N/A	Supported	Design
Admin Search Form Mode	Management > Contribute	Management > Contribute	N/A	N/A	Supported	Design

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Start with a Predefined Search	Management > Contribute	Management > Contribute	N/A	N/A	Supported	Design
Site Collection Features	Management > General Management	Management > General Management	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Supported	Site Collection Administrator
Portal Site Connection	Management > General Management	Management > General Management	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Supported	Site Collection Administrator
Content Type Publishing	Management > General Management	Management > General Management	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Unsupported	Contribute
Web Part	Management > Galleries	Management > Galleries	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Unsupported	Design
Solutions	Management > Galleries	Management > Galleries	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Unsupported	Design
Themes	Management > Galleries	Management > Galleries	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Unsupported	Design
Site Columns	Management > Galleries	Management > Galleries	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Unsupported	Contribute

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Check Broken Link	Management > Check	Management > Check	N/A	N/A	Supported	Unsupported
Search Web Parts	Management > Search Gallery	Management > Search Gallery	N/A	N/A	Supported	Unsupported
Search Duplicate Files	Management > Search Gallery	Management > Search Gallery	N/A	N/A	Supported	Unsupported
Job Monitor	Management > Statistics	Management > Statistics	N/A	N/A	N/A	N/A
Configuration						
Search Setting	Configuration > Search	Unsupported	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Supported	Design
Search Scopes	Configuration > Search	Unsupported	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Unsupported	Site Collection Administrator
Search Keywords	Configuration > Search	Unsupported	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Unsupported	Site Collection Administrator
Quotas and Locks	Configuration > General	Configuration > General	Central Administration > Application Management	Central Administration > Application Management	Supported	Unsupported
Visual Upgrade	Configuration > General	Unsupported	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Unsupported	Unsupported
Deploy Site Maximum Depth	Configuration > General	Configuration > General	N/A	N/A	Supported	Design

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
RSS	Configuration > General	Configuration > General	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Unsupported	Full Control
Help Settings	Configuration > Help	Configuration > Help	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Supported	Site Collection Administrator
SharePoint Designer Settings	Configuration > SharePoint Designer	Configuration > SharePoint Designer	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Supported	Site Collection Administrator
Custom Properties	Configuration > Customization	Configuration > Customization	N/A	N/A	Supported	Unsupported
Security						
People and Groups	Security > Contribute	Security > Contribute	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Unsupported	Site Collection Administrator(Site Owner Group)
Site Permissions	Security > Contribute	Security > Contribute	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Unsupported	Full Control
Security Search Wizard Mode	Security > Contribute	Security > Contribute	N/A	N/A	Supported	Full Control
Security Search Form Mode	Security > Contribute	Security > Contribute	N/A	N/A	Supported	Full Control
Start with a Predefined Search	Security > Contribute	Security > Contribute	N/A	N/A	Supported	Full Control

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Clone User Permissions	Security > Permission	Security > Permission	N/A	N/A	Supported	Full Control
Clone Site Permissions	Security > Permission	Security > Permission	N/A	N/A	Unsupported	Unsupported
Grant Permissions	Security > Permission	Security > Permission	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Supported	Site Collection Administrator
Create Group	Security > Permission	Security > Permission	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Supported	Full Control
Permission Levels	Security > Permission	Security > Permission	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Unsupported	Full Control
Anonymous Access	Security > Permission	Security > Permission	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Supported	Full Control
Export Group for Editing	Security > Permission	Security > Permission	N/A	N/A	Supported	Full Control
Delete Users and Groups	Security > Permission	Security > Permission	N/A	N/A	Supported	Site Collection Administrator
Edit User Permissions	Security > Permission	Security > Permission	Login Site Collection > Site Actions > Site Permissions	Login Site Collection > Settings Icon ⚙ > Site settings > Site Permissions	Supported	Full Control

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Stop Inheriting Permissions – Break Inheritance for Sub-nodes	Security > Permission	Security > Permission	N/A	N/A	Supported	Full Control
Site Collection Administrators	Security > Administrators	Security > Administrators	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Supported	Site Collection Administrator
Primary and Secondary Administrators	Security > Permission	Security > Permission	Central Administration > Application Management	Central Administration > Application Management	Supported	Unsupported
Anonymous Access	Security > Permission	Security > Permission	Login Site Collection > Site Actions > Site Permissions	Login Site Collection > Settings Icon ⚙ > Site settings > Site Permissions	Supported	Full Control
Dead Account Cleaner	Security > Account	Security > Account	N/A	N/A	Supported	Unsupported
Permission Tools Permission Tools						
Grant Permissions	Permission Tools > Grant *Note: After selecting Site Permissions feature, the Permission Tools tab will be enabled.	Permission Tools > Grant *Note: After selecting Site Permissions feature, the Permission Tools tab will be enabled.	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Unsupported	Site Collection Administrator

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Create Group	Permission Tools > Grant	Permission Tools > Grant	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Unsupported	Full Control
Edit User Permissions	Permission Tools > Modify	Permission Tools > Modify	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Supported	Full Control
Remove User Permissions	Permission Tools > Modify	Permission Tools > Modify	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Supported	Full Control
Delete User/Groups from Site Collection	Permission Tools > Modify	Permission Tools > Modify	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Supported	Site Collection Administrator
Anonymous Access	Permission Tools > Manage	Permission Tools > Manage	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	N/A	Full Control
Permission Levels	Permission Tools > Manage	Permission Tools > Manage	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	N/A	Full Control
Site Collection Administrators	Permission Tools > Manage	Permission Tools > Manage	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	N/A	Site Collection Administrator
Grant Temporary Permissions	Security > Permission	Security > Permission	N/A	N/A	Supported	Unsupported

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Search Temporary Permissions	Security > Permission	Security > Permission	N/A	N/A	Supported	Unsupported
Policy Enforcer						
Create or Apply Profile	Policy Enforcer > Policy Enforcer	Policy Enforcer > Policy Enforcer	N/A	N/A	Supported	Unsupported
Profile Manager	Policy Enforcer > Policy Enforcer	Policy Enforcer > Policy Enforcer	N/A	N/A	Unsupported	Unsupported
Generate Report	Policy Enforcer > Report	Policy Enforcer > Report	N/A	N/A	Supported	Unsupported
Source Management	Policy Enforcer > Settings	Policy Enforcer > Settings	N/A	N/A	Unsupported	Unsupported
Policy Enforcer Database	Policy Enforcer > Settings	Policy Enforcer > Settings	N/A	N/A	Unsupported	Unsupported
Filter Policy	Policy Enforcer > Settings	Policy Enforcer > Settings	N/A	N/A	Unsupported	Unsupported

Sub-Site Level Operations

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Management						
New Sub-site	Management > Contribute	Management > Contribute	Login a Site > Site Actions > New Site	Login a Site > Site Contents > new sub-site	Supported	Full Control
New List\Library	Management > Contribute	Management > Contribute	Login a Site > Site Actions > More Options	Login a Site > Settings Icon ⚙ > Add an app	Supported	Design
Delete	Management > Contribute	Management > Contribute	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Supported	Full Control
Admin Search Wizard Mode	Management > Contribute	Management > Contribute	N/A	N/A	Supported	Design permission for both current node and parent node
Admin Search Form Mode	Management > Contribute	Management > Contribute	N/A	N/A	Supported	Design permission for both current node and parent node
Start with a Predefined Search	Management > Contribute	Management > Contribute	N/A	N/A	Supported	Design permission for both current node and parent node
Site Features	Management > General Management	Management > General Management	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Supported	Full Control
Reset To Site Definition	Management > General Management	Management > General Management	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Unsupported	Unsupported

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Regional Settings	Management > General Management	Management > General Management	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Supported	Full Control
Site Columns	Management > Galleries	Management > Galleries	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Unsupported	Contribute
Site Content Types	Management > Galleries	Management > Galleries	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Unsupported	Contribute
Master Page	Management > Galleries	Management > Galleries	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Unsupported	Contribute
Check Broken Link	Management > Check	Management > Check	N/A	N/A	Supported	Unsupported
Search Web Parts	Management > Search Gallery	Management > Search Gallery	N/A	N/A	Supported	Unsupported
Search Duplicate Files	Management > Search Gallery	Management > Search Gallery	N/A	N/A	Supported	Unsupported
Job Monitor	Management > Statistics	Management > Statistics	N/A	N/A	N/A	Unsupported
Configuration						
RSS Setting	Configuration > General	Configuration > General	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Unsupported	Unsupported
Search And Offline Availability	Configuration > General	Configuration > General	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Supported	Full Control

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Related Links Scope Settings	Configuration > General	Unsupported	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Unsupported	Unsupported
Title, Description, and Icon	Configuration > Look and Feel	Configuration > Look and Feel	Login a Site > Site Actions > Site Settings	Login a Site > Site Actions > Site Settings	Unsupported	Full Control
Quick Launch	Configuration > Look and Feel	Configuration > Look and Feel	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Unsupported	Design
Top Link Bar	Configuration > Look and Feel	Configuration > Look and Feel	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Unsupported	Design
Tree View	Configuration > Look and Feel	Configuration > Look and Feel	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Unsupported	Full Control
Site Theme (As "Change the Look" in DocAve when specifying the site on the SharePoint 2013 farm)	Configuration > Look and Feel	Configuration > Look and Feel	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Supported	Design
Custom Properties	Configuration > Customization	Configuration > Customization	N/A	N/A	Supported	Unsupported
Security						
People and Groups	Security > Contribute	Security > Contribute	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Unsupported	Contribute

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Site Permissions	Security > Contribute	Security > Contribute	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Unsupported	Full Control
Security Search Wizard Mode	Security > Contribute	Security > Contribute	N/A	N/A	Supported	Design permission for parent node and Full Control permission for current node
Security Search Form Mode	Security > Contribute	Security > Contribute	N/A	N/A	Supported	Design permission for parent node and Full Control permission for current node
Start with a Predefined Search	Security > Contribute	Security > Contribute	N/A	N/A	Supported	Design permission for parent node and Full Control permission for current node
Clone User Permissions	Security > Permission	Security > Permission	N/A	N/A	Supported	Site Collection Administrator
Clone Site Permissions	Security > Permission	Security > Permission	N/A	N/A	Unsupported	Unsupported
Grant Permissions	Security > Permission	Security > Permission	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Supported	Site Collection Administrator
Create Group	Security > Permission	Security > Permission	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Supported	Full Control

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Permission Levels	Security > Permission	Security > Permission	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Unsupported	Full Control
Anonymous Access	Security > Permission	Security > Permission	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Supported	Full Control
Stop Inheriting Permissions – Break Inheritance for Selected Node	Security > Permission	Security > Permission	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Supported	Full Control
Stop Inheriting Permissions – Break Inheritance for Sub-nodes	Security > Permission	Security > Permission	Unsupported	Unsupported	Supported	Design permission for parent node and Full Control permission for current node
Inherit Permissions	Security > Permission	Security > Permission	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Supported	Full Control
Edit User Permissions	Security > Permission	Security > Permission	Login a Site > Site Actions > Site Permissions	Login a Site > Settings Icon ⚙ > Site settings > Site Permissions	Supported	Full Control
User Alerts	Security > Share and Track	Security > Share and Track	Login a Site > Site Actions > Site Settings	Login a Site > Settings Icon ⚙ > Site settings	Unsupported	Unsupported
Search Alert	Security > Share and Track	Security > Share and Track	N/A	N/A	Unsupported	Unsupported
Dead Account Cleaner	Security > Account	Security > Account	N/A	N/A	Supported	Unsupported

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Permission Tools						
Grant Permissions	Permission Tools > Grant *Note: after selecting Site Permissions feature, the Permission Tools tab will be enabled.	Permission Tools > Grant *Note: after selecting Site Permissions feature, the Permission Tools tab will be enabled.	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Supported	Site Collection Administrator
Create Group	Permission Tools > Grant	Permission Tools > Grant	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Supported	Full Control
Inherit Permissions	Permission Tools > Inheritance	Permission Tools > Inheritance	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	N/A	Full Control
Stop Inheriting Permissions– Break Inheritance for Selected Node	Permission Tools > Inheritance	Permission Tools > Inheritance	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	N/A	Full Control
Stop Inheriting Permissions – Break Inheritance for Sub-nodes	Permission Tools > Inheritance	Permission Tools > Inheritance	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	N/A	Full Control

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Edit User Permissions	Permission Tools > Modify	Permission Tools > Modify	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Supported	Full Control
Remove User Permissions	Permission Tools > Modify	Permission Tools > Modify	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	Supported	Full Control
Permission Levels	Permission Tools > Manage	Permission Tools > Manage	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	N/A	Full Control
Grant Temporary Permissions	Security > Permission	Security > Permission	N/A	N/A	Supported	Unsupported
Search Temporary Permissions	Security > Permission	Security > Permission	N/A	N/A	Supported	Unsupported
Policy Enforcer						
Create or Apply Profile	Policy Enforcer > Policy Enforcer	Policy Enforcer > Policy Enforcer	N/A	N/A	Supported	Unsupported
Profile Manager	Policy Enforcer > Policy Enforcer	Policy Enforcer > Policy Enforcer	N/A	N/A	Unsupported	Unsupported
Generate Report	Policy Enforcer > Report	Policy Enforcer > Report	N/A	N/A	Supported	Unsupported
Source Management	Policy Enforcer > Settings	Policy Enforcer > Settings	N/A	N/A	Unsupported	Unsupported
Policy Enforcer Database	Policy Enforcer > Settings	Policy Enforcer > Settings	N/A	N/A	Unsupported	Unsupported

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Filter Policy	Policy Enforcer > Settings	Policy Enforcer > Settings	N/A	N/A	Unsupported	Unsupported

List/Library Level Operations

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Management						
New Folder	Management > Contribute	Management > Contribute	Access a library > Documents > New Folder	Access a library > FILES > New Folder	Supported	Contribute
Delete	Management > Contribute	Management > Contribute	Access a list/library > List/Library > List/Library Settings	Access a list/library > LIST/LIBRARY > List/Library Settings	Supported	Design
Admin Search Wizard Mode	Management > Contribute	Management > Contribute	N/A	N/A	Supported	Design permission for both current node and parent node
Admin Search Form Mode	Management > Contribute	Management > Contribute	N/A	N/A	Supported	Design permission for both current node and parent node
Start with a Predefined Search	Management > Contribute	Management > Contribute	N/A	N/A	Supported	Design permission for both current node and parent node

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
No checked In Version Files	Management > General Management	Management > General Management	Access a library > Library > Library Settings	Access a library > LIBRARY > Library Settings	Unsupported	Unsupported
Workflow Settings	Management > General Management	Management > General Management	Access a list/library > List/Library	Access a list/library > LIST/LIBRARY	Unsupported	Unsupported
Metadata and Keywords Settings	Management > General Management	Management > General Management	Access a list/library > List/Library > List/Library Settings	Access a list/library > LIST/LIBRARY > List/Library Settings	Unsupported	Design permission for parent node and Full Control permission for current node
Information management policy settings	Management > General Management	Management > General Management	Access a list/library > List/Library > List/Library Settings	Access a list/library > LIST/LIBRARY > List/Library Settings	Supported	
Indexed Columns	Management > Columns	Management > Columns	Access a list/library > List/Library > List/Library Settings	Access a list/library > LIST/LIBRARY > List/Library Settings	Unsupported	Unsupported
Job Monitor	Management > Statistics	Management > Statistics	N/A	N/A	N/A	N/A
Configuration						
Versioning Settings	Configuration > General	Configuration > General	Access a list/library > List/Library > List/Library Settings	Access a list/library > LIST/LIBRARY > List/Library Settings	Supported	Design (does not support version)

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Advanced Settings	Configuration > General	Configuration > General	Access a list/library > List/Library > List/Library Settings	Access a list/library > LIST/LIBRARY > List/Library Settings	Supported	Design
Validation Settings	Configuration > General	Configuration > General	Access a list/library > List/Library > List/Library Settings	Access a list/library > LIST/LIBRARY > List/Library Settings	Unsupported	Design
Column Default Value Settings	Configuration > General	Configuration > General	Access a library > Library > Library Settings	Access a library > LIBRARY > Library Settings	Unsupported	Unsupported
Rating Settings	Configuration > General	Configuration > General	Access a list/library > List/Library > List/Library Settings	Access a list/library > LIST/LIBRARY > List/Library Settings	Supported	Design
Audience Targeting Settings	Configuration > General	Configuration > General	Access a list/library > List/Library > List/Library Settings	Access a list/library > LIST/LIBRARY > List/Library Settings	Unsupported	Design
Metadata Navigation Settings	Configuration > General	Unsupported	Access a list/library > List/Library > List/Library Settings	Access a list/library > LIST/LIBRARY > List/Library Settings	Unsupported	Design

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Pre-location View Settings	Configuration > General	Unsupported	Access a list/library > List/Library > List/Library Settings	Access a list/library > LIST/LIBRARY > List/Library Settings	Unsupported	Unsupported
RSS Setting	Configuration > General	Configuration > General	Access a list/library > List/Library > List/Library Settings	Access a list/library > LIST/LIBRARY > List/Library Settings	Unsupported	Unsupported
Title, Description and Navigation	Configuration > Look and Feel	Configuration > Look and Feel	Access a list/library > List/Library > List/Library Settings	Access a list/library > LIST/LIBRARY > List/Library Settings	Unsupported	Design
Security						
List Permissions	Security > Contribute	Security > Contribute	Access a list/library > List/Library > List/Library Permissions	Access a list/library > LIST/LIBRARY > List/Library Settings > Permissions and Management	Unsupported	Full Control
Security Search Wizard Mode	Security > Contribute	Security > Contribute	N/A	N/A	Supported	Design permission for parent node and Full Control permission for current node

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Security Search Form Mode	Security > Contribute	Security > Contribute	N/A	N/A	Supported	Design permission for parent node and Full Control permission for current node
Start with a Predefined Search	Security > Contribute	Security > Contribute	N/A	N/A	Supported	Design permission for parent node and Full Control permission for current node
Clone User Permissions	Security > Permission	Security > Permission	N/A	N/A	Supported	Site Collection Administrator
Clone List/Library Permissions	Security > Permission	Security > Permission	N/A	N/A	Unsupported	Unsupported
Grant Permissions	Security > Permission	Security > Permission	Access a list/library > List/Library > List/Library Permissions	Access a list/library > LIST/LIBRARY > List/Library Settings > Permissions and Management	Supported	Site Collection Administrator
Grant Temporary Permissions	Security > Permission	Security > Permission	N/A	N/A	Supported	Unsupported

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Search Temporary Permissions	Security > Permission	Security > Permission	N/A	N/A	Supported	Unsupported
Anonymous Access	Security > Permission	Security > Permission	Access a list/library > List/Library > List/Library Permissions	Access a list/library > LIST/LIBRARY > List/Library Settings > Permissions and Management	Supported	Full Control
Stop Inheriting Permissions – Break Inheritance for Selected Node	Security > Permission	Security > Permission	Access a list/library > List/Library > List/Library Permissions	Access a list/library > LIST/LIBRARY > List/Library Settings > Permissions and Management	Supported	Full Control
Stop Inheriting Permissions – Break Inheritance for Sub-nodes	Security > Permission	Security > Permission	N/A	N/A	Supported	Design permission for parent node and Full Control permission for current node

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Inherit Permissions – Apply Inheritance to Selected Node	Security > Permission	Security > Permission	Access a list/library > List/Library > List/Library Permissions	Access a list/library > LIST/LIBRARY > List/Library Settings > Permissions and Management	Supported	Full Control
Inherit Permissions – Push Inheritance for Sub-nodes	Security > Permission	Security > Permission	N/A	N/A	Supported	Design permission for parent node and Full Control permission for current node
Start alert on this library/list	Security > Share and Track	Security > Share and Track	Access a list/library > List/Library > Alert Me	Access a list/library > LIST/LIBRARY > Alert Me	Supported	Unsupported
Manage My Alert	Security > Share and Track	Security > Share and Track	Access a list/library > List/Library > Alert Me	Access a list/library > LIST/LIBRARY > Alert Me	Unsupported	Unsupported
Permission Tools						
Inherit Permissions	Permission Tools > Inheritance ***Note**: after selecting List Permissions feature, the Permission Tools tab will be enabled.	Permission Tools > Inheritance ***Note**: after selecting List Permissions feature, the Permission Tools tab will be enabled.	Access a list/library > List/Library > List/Library Permissions	Access a list/library > LIST/LIBRARY > List/Library Settings > Permissions and Management	N/A	Full Control

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Stop Inheriting Permissions– Break Inheritance for Selected Node	Permission Tools > Inheritance	Permission Tools > Inheritance	Access a list/library > List/Library > List/Library Permissions	Access a list/library > LIST/LIBRARY > List/Library Settings > Permissions and Management	N/A	Full Control
Stop Inheriting Permissions – Break Inheritance for Sub-nodes	Permission Tools > Inheritance	Permission Tools > Inheritance	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	N/A	Full Control
Grant Permissions	Permission Tools > Grant	Permission Tools > Grant	Access a list/library > List/Library > List/Library Permissions	Access a list/library > LIST/LIBRARY > List/Library Settings > Permissions and Management	Supported	Site Collection Administrator
Edit User Permissions	Permission Tools > Modify	Permission Tools > Modify	Access a list/library > List/Library > List/Library Permissions	Access a list/library > LIST/LIBRARY > List/Library Settings > Permissions and Management	Supported	Full Control

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Remove User Permissions	Permission Tools > Modify	Permission Tools > Modify	Access a list/library > List/Library > List/Library Permissions	Access a list/library > LIST/LIBRARY > List/Library Settings > Permissions and Management	Supported	Full Control

Folder Level Operations

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Management						
New Folder	Management > Contribute	Management > Contribute	Access a folder > Documents > New Folder	Access a folder > FILES > New Folder	Supported	Design permission for both current node and parent node
Delete	Management > Contribute	Management > Contribute	Select a folder > Documents > Delete	Select a folder > FILES > Delete	Supported	Design permission for both current node and parent node
Admin Search Wizard Mode	Management > Contribute	Management > Contribute	N/A	N/A	Supported	Design permission for both current node and parent node
Admin Search Form Mode	Management > Contribute	Management > Contribute	N/A	N/A	Supported	Design permission for both current node and parent node
Start with a Predefined Search	Management > Contribute	Management > Contribute	N/A	N/A	Supported	Design permission for both current node and parent node

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
View Properties	Management > Contribute	Management > Contribute	Select a folder > Documents > View Properties	Select a folder > FILES > View Properties	Supported	Design permission for both current node and parent node
Job Monitor	Management > Statistics		N/A	N/A	N/A	N/A
View Properties						
Edit	View Properties > Management *Note: After selecting View Properties feature, the tab is enabled.	View Properties > Management *Note: After selecting View Properties feature, the tab is enabled.	Select a folder > Documents > Edit Properties	Select a folder > FILES > Edit Properties	Unsupported	Design permission for parent node and Full Control permission for current node
Security						
Folder Permissions	Security > Contribute	Security > Contribute	N/A	N/A	Unsupported	Design permission for parent node and Full Control permission for current node
Security Search Wizard Mode	Security > Contribute	Security > Contribute	N/A	N/A	Supported	Design permission for parent node and Full Control permission for current node

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Security Search Form Mode	Security > Contribute	Security > Contribute	N/A	N/A	Supported	Design permission for parent node and Full Control permission for current node
Start with a Predefined Search	Security > Permission	Security > Permission	N/A	N/A	Supported	Design permission for parent node and Full Control permission for current node
Clone User Permissions	Security > Permission	Security > Permission	N/A	N/A	Supported	Site Collection Administrator
Clone Folder Permissions	Security > Permission	Security > Permission	Select a folder > Documents > Document Permissions	Select a folder > Documents > Document Permissions	Unsupported	Unsupported
Grant Permissions	Security > Permission	Security > Permission	Select a folder > Documents > Document Permissions	Select a folder > Documents > Document Permissions	Supported	Site Collection Administrator
Stop Inheriting Permissions – Break Inheritance for Selected Node	Security > Permission	Security > Permission	N/A	N/A	Supported	Design permission for parent node and Full Control permission for current node

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Stop Inheriting Permissions – Break Inheritance for Sub-nodes	Security > Permission	Security > Permission	Select a folder > Documents > Document Permissions	Select a folder > Documents > Document Permissions	Supported	Design permission for parent node and Full Control permission for current node
Inherit Permissions – Apply Inheritance to Selected Node	Security > Permission	Security > Permission	N/A	N/A	Supported	Design permission for parent node and Full Control permission for current node
Inherit Permissions – Push Inheritance for Sub-nodes	Security > Alert	Security > Alert	Select a folder > Documents > Alert Me	Select a folder > Documents > Alert Me	Supported	Design permission for parent node and Full Control permission for current node
Alert Me	Security > Alert	Security > Alert	Select a folder > Documents > Alert Me	Select a folder > Documents > Alert Me	Supported	Unsupported
Inherit Permissions	Permission Tools > Inheritance	Permission Tools > Inheritance	Select a folder > Documents > Document Permissions	Select a folder > Documents > Document Permissions	N/A	Design permission for parent node and Full Control permission for current node

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Stop Inheriting Permissions– Break Inheritance for Selected Node	Permission Tools > Inheritance	Permission Tools > Inheritance	Login Site Collection > Site Actions > Site Settings	Login Site Collection > Settings Icon ⚙ > Site settings	N/A	Design permission for parent node and Full Control permission for current node
Stop Inheriting Permissions – Break Inheritance for Sub-nodes	Permission Tools > Grant	Permission Tools > Grant	Select a folder > Documents > Document Permissions	Select a folder > Documents > Document Permissions	N/A	Full Control
Grant Permissions	Permission Tools > Modify	Permission Tools > Modify	Select a folder > Documents > Document Permissions	Select a folder > Documents > Document Permissions	Supported	Site Collection Administrator
Edit User Permissions	Permission Tools > Modify	Permission Tools > Modify	Select a folder > Documents > Document Permissions	Select a folder > Documents > Document Permissions	Supported	Design permission for parent node and Full Control permission for current node
Remove User Permissions	Permission Tools > Modify	Permission Tools > Modify	Select a folder > Documents > Document Permissions	Select a folder > Documents > Document Permissions	Supported	Design permission for parent node and Full Control permission for current node

Item Level Operations

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Management						
Delete	Management > Contribute	Management > Contribute	Select an item > Items > Delete Item	Select an item > FILES > Delete Item	Supported	Design permission for both parent node and current node
Admin Search Wizard Mode	Management > Contribute	Management > Contribute	N/A	N/A	Supported	Design permission for both parent node and current node
Admin Search Form Mode	Management > Contribute	Management > Contribute	N/A	N/A	Supported	Design permission for both parent node and current node
Start with a Predefined Search	Management > Contribute	Management > Contribute	N/A	N/A	Supported	Design permission for both parent node and current node
Change Metadata	Management > Action	Management > Action	N/A	N/A	Supported	Unsupported
Job Monitor	Management > Statistics	Management > Statistics	N/A	N/A	N/A	N/A
Security						
Item Permissions – Apply Inheritance to Selected Node	Security > Contribute	Security > Contribute	Select an item > Items > Item Permissions	Select an item > Items > Item Permissions	Unsupported	Design permission for parent node and own Full Control to the items
Security Search Wizard Mode	Security > Contribute	Security > Contribute	N/A	N/A	Supported	Design permission for parent node and own Full Control to the items

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Security Search Form Mode	Security > Contribute	Security > Contribute	N/A	N/A	Supported	Design permission for parent node and own Full Control to the items
Start with a Predefined Search	Security > Contribute	Security > Contribute	N/A	N/A	Supported	Design permission for parent node and own Full Control to the items
Stop Inheriting Permissions– Break Inheritance for Selected Node	Security > Permission	Security > Permission	Select an item > Items > Item Permissions	Select an item > Items > Item Permissions	Supported	Design permission for parent node and own Full Control to the items
Inherit Permissions	Security > Permission	Security > Permission	Select an item > Items > Item Permissions	Select an item > Items > Item Permissions	Supported	Design permission for parent node and own Full Control to the items
Grant Permissions	Security > Permission	Security > Permission	Select an item > Items > Item Permissions	Select an item > Items > Item Permissions	Supported	Site Collection Administrator
Alert Me	Security > Alert	Security > Alert	Select an item > Items > Alert Me	Select an item > Items > Alert Me	Supported	Unsupported
Permission Tools						
Inherit Permissions	Permission Tools > Inheritance *Note: Selecting Item Permissions enables Permission Tools tab.	Permission Tools > Inheritance *Note: Selecting Item Permissions enables Permission Tools tab.	Select an item > Items > Item Permissions	Select an item > Items > Item Permissions	N/A	Design permission for parent node and own Full Control to the items

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Stop Inheriting Permissions – Break Inheritance for Selected Node	Permission Tools > Inheritance	Permission Tools > Inheritance	Select an item > Items > Item Permissions	Select an item > Items > Item Permissions	N/A	Design permission for parent node and own Full Control to the items
Grant Permissions	Permission Tools > Grant	Permission Tools > Grant	Select an item > Items > Item Permissions	Select an item > Items > Item Permissions	Supported	Site Collection Administrator
Edit User Permissions	Permission Tools > Modify	Permission Tools > Modify	Select an item > Items > Item Permissions	Select an item > Items > Item Permissions	Supported	Design permission for parent node and own Full Control to the items
Remove User Permissions	Permission Tools > Modify	Permission Tools > Modify	Select an item > Items > Item Permissions	Select an item > Items > Item Permissions	Supported	Design permission for parent node and own Full Control to the items

Appendix C: Security Search Result

Refer to the table below for more information about the functions that are available to the Security Search results.

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Search Result Tools (Groups)						
Add Users	Search Result Tools > Contribute	Search Result Tools > Contribute	N/A	N/A	Supported	Site Collection Administrator
Group Settings	Search Result Tools > Contribute	Search Result Tools > Contribute	N/A	N/A	Supported	Site Collection Administrator
Edit Group Permissions	Search Result Tools > Contribute	Search Result Tools > Contribute	N/A	N/A	Supported	Full Control
Remove Group Permissions	Search Result Tools > Contribute	Search Result Tools > Contribute	N/A	N/A	Supported	Full Control
Clone User Permissions	Search Result Tools > Contribute	Search Result Tools > Contribute	N/A	N/A	Unsupported	Full Control
Dead Account Cleaner	Search Result Tools > Contribute	Search Result Tools > Contribute	N/A	N/A	Supported	Unsupported
Download Report	Job Monitor > Download Report or Search Result Tools > Export and Import	Job Monitor > Download Report or Search Result Tools > Export and Import	N/A	N/A	N/A	Full Control
Export for Editing	Job Monitor > Export for Editing or Search Result Tools > Export and Import	Job Monitor > Export for Editing or Search Result Tools > Export and Import	N/A	N/A	N/A	Full Control
Import Configuration File	Search Result Tools > Export and Import	Search Result Tools > Export and Import	N/A	N/A	N/A	Unsupported
Permission Level	Search Result Tools > Permission Level column	Search Result Tools > Permission Level column	N/A	N/A	N/A	Full Control

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Search Result Tools (User)						
Edit User Permissions	Search Result Tools > Contribute		N/A	N/A		Full Control
Remove User Permissions	Search Result Tools > Contribute		N/A	N/A	Supported	Full Control
Delete Users	Search Result Tools > Contribute		N/A	N/A	Supported	Full Control
Clone User Permissions	Search Result Tools > Contribute		N/A	N/A	Unsupported	Full Control
Download Report	Search Result Tools > Export and Import		N/A	N/A	N/A	Full Control
Export for Editing	Search Result Tools > Export and Import		N/A	N/A	N/A	Full Control
Import Configuration File	Search Result Tools > Export and Import		N/A	N/A	N/A	Unsupported
Search Result Tools (Site Collection Administrator)						
Site Collection Administrators	Search Result Tools > Contribute	Search Result Tools > Contribute	Login Site Collection > Site Actions > Site Permissions	Login Site Collection > Settings Icon ⚙ > Site settings > Site Permissions	Supported	Site Collection Administrator

Operation	Location in DocAve (SharePoint 2010)	Location in DocAve (SharePoint 2013)	Location in SharePoint 2010	Location in SharePoint 2013	Batch Settings	Minimum Permission
Primary and Secondary Administrators	Search Result Tools > Contribute	Search Result Tools > Contribute	Central Administration > Application Management	Central Administration > Application Management	Supported	Unsupported
Download Report	Search Result Tools > Export and Import	Search Result Tools > Export and Import	N/A	N/A	N/A	Full Control
Export for Editing	Search Result Tools > Export and Import	Search Result Tools > Export and Import	N/A	N/A	N/A	Full Control
Import Configuration File	Search Result Tools > Export and Import	Search Result Tools > Export and Import	N/A	N/A	N/A	Unsupported

Appendix D: Feature Updates in DocAve when Specifying Nodes on the SharePoint 2013 Farm

DocAve 6 Service Pack 2 updates the features which are provided in SharePoint 2013. Refer to the following table to view the features update.

Function	Level	Location in DocAve (SharePoint 2013)	Location in SharePoint 2013
Checkbox "Check this box in multi-tenant Con Configurations to allow tenants to configure tenant level IRM settings"	Farm	Security > Select a farm > Information Policy > Configure Information Rights Management	Central Administration > Application Management > Select a web application > General Settings > General Settings
Select Experience Version	Web Application	Management > Select a web application > Contribute > New > New Site Collection	Central Administration > Application Management > Create site collections
User Settings Provider	Web Application	Management > Manage > General Settings > General Settings	Central Administration > Application Management > Select a web application > General Settings > General Settings
Usage Cookie	Web Application	Management > Manage > General Settings > General Settings	Central Administration > Application Management > Select a web application > General Settings > General Settings
Site collection administrator controlled read-only lock (Archived)	Site Collection	Configuration > Select a site collection > General > Quotas and Locks	Central Administration > Application Management > Configure quotas and locks
Farm administrator controlled read-only lock	Site Collection	Configuration > Select a site collection > General > Quotas and Locks	Central Administration > Application Management > Configure quotas and locks
Set Up Groups for this Site	Site	Select Use unique permissions before creating a new subsite on the site collection level. Click **Create** to redirect to the **Set Up Groups for this Site** page.	Access a Site > Select Site Contents > new subsite > Create without selecting Use unique permissions.

Function	Level	Location in DocAve (SharePoint 2013)	Location in SharePoint 2013
		If creating a new sub site without using unique permissions, select this new created site and navigate to Security > Permission > Stop Inheriting Permissions > Break Inheritance for Selected Node	
Reindex Site	Site	Configuration > Select a site > General > Search and Offline Availability	Access a Site > Settings Icon ⚙ > Site settings > Search and offline availability
Reindex List/Library	List/Library	Configuration > Select a list/library > General > Advanced Settings	Access a list/library > LIST/LIBRARY > List/Library Settings > Advance settings
Rate Settings ("Likes" and "Star Ratings")	List/Library	Configuration > Select a list/library > General > General Settings > Rating Settings	Access a list/library > LIST/LIBRARY > List/Library Settings > Rating Settings

Note: The function **Set Up Groups for this Site** can also be applied at site level on the SharePoint 2010 farm.

Appendix E: Administrator Configuration File

On the SharePoint 2010 server with DocAve Manager installed, DocAve Administrator provides two configuration files named **CentralAdminDuplicateFilesExtensions.xml** and **CentralAdminDuplicateFilesCommonFileNames2010.xml**, which allowing you to modify some default settings for the **Search Duplicate Files** function.

On the SharePoint 2013 server with DocAve Manager installed, the corresponding configuration files named **CentralAdminDuplicateFilesExtensions.xml** and **CentralAdminDuplicateFilesCommonFileNames2013.xml** are provided and used the same way as on the SharePoint 2010 server.

The two configuration files reside in **C:\Program Files\AvePoint\DocAve6\Manager\Control\Config\CentralAdmin** by default.

Configuring CentralAdminDuplicateFilesExtensions.xml

A search criterion called **Include file extension only** is available while setting up the Search Duplicate Files plan in DocAve Administrator. You can specify the file types to be searched in the **Include file extension only** drop-down list. All the file extensions displayed in this drop-down list are stored in the **CentralAdminDuplicateFilesExtensions.xml** file. You are able to add new file extensions or remove existing file extensions from this configuration file to control the file extensions that can be displayed in the **Include file extension only** drop-down list.

For the **CentralAdminDuplicateFilesExtensions.xml** file on the SharePoint 2013 server, the configuration method is the same as one used on the SharePoint 2010 server.

Configuring CentralAdminDuplicateFilesCommonFileNames2010.xml

A search criterion called **Exclude file** is available while setting up the Search Duplicate Files plan in DocAve Administrator. You can specify the file that will be excluded in the search scope in the **Exclude file** drop-down list. All the files displayed in this drop-down list are stored in the **CentralAdminDuplicateFilesCommonFileNames2010.xml** file. You are able to add new files or remove existing files from this configuration file to control the files that can be displayed in the **Exclude file** drop-down list.

For the **CentralAdminDuplicateFilesCommonFileNames2013.xml** file on the SharePoint 2013 server, the configuration method is the same as one used on the SharePoint 2010 server.

Appendix F: Supported and Unsupported List of DocAve Administrator Functions for SharePoint Online

Some DocAve Administrator functions are unique to DocAve, while some functions also available in SharePoint Online. Refer to the tables below for more information.

Site Collection Level Operations

Refer to the table below for information about supported and unsupported functions at the site collection level.

*Note: Some cells in the tables below indicate partial support. For details on unsupported options, refer to Unsupported Functionalities for Office 365 or Remote Farms.

Tab	Group	Function	SharePoint 2010 Online	SharePoint 2013 Online
Management	Contribute	New (Site)	Supported	Supported
		Move	Unsupported	Unsupported
		Delete	Unsupported	Unsupported
		Admin Search > Admin Search Wizard Mode	Supported	Supported
		Admin Search > Admin Search Form Mode	Supported	Supported
		Admin Search > Start with a Predefined Search	Supported	Supported
	General Management	Site Collection Features	Supported	Supported
		Portal Site Connection	Supported	Supported
		Content Type Publishing	Supported	Supported
	Galleries	Web Part	Supported	Supported
		Themes	Supported	Supported
		Solutions	Supported	Supported
		Site Columns	Supported	Supported
	Check	Check Broken Link	Unsupported	Unsupported
	Search Gallery	Search Web Part	Unsupported	Unsupported
		Search Duplicate Files	Unsupported	Unsupported
	Statistics	Job Monitor	Supported	Supported
Configuration	Search	Search Settings > Search Setting	Supported	Supported
		Search Settings > Search Scope	Supported	Supported
		Search Settings > Search Keywords	Supported	Supported
	General	Quotas and Locks	Unsupported	Unsupported

Tab	Group	Function	SharePoint 2010 Online	SharePoint 2013 Online
		Deploy Site Maximum Depth	Supported	Supported
		Visual Upgrade	Unsupported	Unsupported
		RSS	Supported	Supported
	Help	Help Settings	Supported	Supported
	SharePoint	SharePoint Designer Settings	Supported	Supported
	Customization	Custom Properties	Unsupported	Unsupported
Security	Contribute	Users and Permissions > People and Groups	Supported	Supported
		Users and Permissions > Site Permissions	Supported	Supported
		Security Search > Security Search Wizard Mode	Supported	Supported
		Security Search > Security Search Form Mode	Supported	Supported
		Security Search > Start with a Predefined Search	Supported	Supported
	Permission	Clone Permission > Clone User Permissions	Supported	Supported
		Clone Permission > Clone Site Permission	Unsupported	Unsupported
		Grant Permissions	Supported	Supported
		Create Group	Supported	Supported
		Edit User Permissions	Supported	Supported
		Delete Users and Groups	Supported	Supported
		Stop inheriting Permissions > Break Inheritance for Sub-nodes	Supported	Supported
		Permission Levels	Supported	Supported
		Anonymous Access	Unsupported	Unsupported
		Export Group For Editing	Supported	Supported
		Site Collection Administrators > Site Collection Administrator	Supported	Supported
		Site Collection Administrators > Primary and Secondary Administrator	Unsupported	Unsupported
	Account	Dead Account Cleaner > Plan Mode	Unsupported	Unsupported
		Dead Account Cleaner > Scan Mode	Unsupported	Unsupported
	Statistics	Job Monitor	Supported	Supported

Tab	Group	Function	SharePoint 2010 Online	SharePoint 2013 Online
Permission Tools	Grant	Grant Permissions	Supported	Supported
		Create Group	Supported	Supported
	Modify	Edit User Permissions	Supported	Supported
		Remove User Permissions	Supported	Supported
		Delete User/Groups from Site Collection	Supported	Supported
	Manage	Permission Levels	Supported	Supported
		Anonymous Access	Unsupported	Unsupported
		Site Collection Administrators > Site Collection Administrator	Supported	Supported
Users and Permissions	People and Groups	All people > Delete User from Site Collection	Supported	Supported
		Group > New Group	Supported	Supported
		Group > Edit Group Setting	Supported	Supported
		Add users	Supported	Supported
		Remove User from Group	Supported	Supported
		Group settings	Supported	Supported
Policy Enforcer	All groups	All functions	Supported	Supported

Site Level Operations

Refer to the table below for the information about the supported and unsupported functions at the site level.

*Note: Some cells in the tables below indicate partial support. For details on unsupported options, refer to [Unsupported Functionalities for Office 365 or Remote Farms.](#)

Tab	Group	Function	SharePoint 2010 Online	SharePoint 2013 Online
Management	Contribute	New > New Subsite	Supported	Supported
		New > New List/Library	Supported	Supported
		Admin Search > Admin Search Wizard Mode	Supported	Supported
		Admin Search > Admin Search Form Mode	Supported	Supported
		Admin Search > Start with a Predefined Search	Supported	Supported
		Delete	Supported	Supported
	General Management	Site Features	Supported	Supported
		Reset To Site Definition	Supported	Supported
		Regional Settings	Supported	Supported
	Galleries	Site Columns	Supported	Supported

Tab	Group	Function	SharePoint 2010 Online	SharePoint 2013 Online
		Site Content Types	Supported	Supported
		Master Page	Supported	Supported
	Check	Check Broken Link	Unsupported	Unsupported
	Search Gallery	Search Web Part	Unsupported	Unsupported
		Search Duplicate Files	Unsupported	Unsupported
	Statistics	Job Monitor	Supported	Supported
Configuration	General	RSS Setting	Supported	Supported
		Search And Offline Availability	Supported	Supported
		Related Links Scope Settings	Unsupported	Unsupported
	Look and Feel	Title, Description, and Icon	Supported	Supported
		Quick Launch	Supported	Supported
		Top Link Bar	Supported	Supported
		Tree View	Supported	Supported
		Site Theme	Supported	Supported
	Customization	Custom Properties	Unsupported	Unsupported
Security	Contribute	Users and Permissions > People and Groups	Supported	Supported
		Users and Permissions > Site Permissions	Supported	Supported
		Security Search > Security Search Wizard Mode	Supported	Supported
		Security Search > Security Search Form Mode	Supported	Supported
		Security Search > Start with a Predefined Search	Supported	Supported
	Permission	Clone Permission > Clone User Permissions	Unsupported	Unsupported
		Clone Permission > Clone Site Permission	Unsupported	Unsupported
		Grant Permissions	Supported	Supported
		Create Group	Supported	Supported
		Edit User Permissions	Unsupported	Unsupported
		Anonymous Access	Unsupported	Unsupported
		Permission levels	Supported	Supported
		Stop inheriting Permissions > Break Inheritance for Selected Nodes	Supported	Supported
		Stop inheriting Permissions > Break Inheritance for Sub-nodes	Supported	Supported
		Inherit Permissions	Supported	Supported
	Share and	Alert Me > User Alert	Unsupported	Unsupported

DocAve 6: Administrator

Tab	Group	Function	SharePoint 2010 Online	SharePoint 2013 Online
	Track	Alert Me > Search Alert	Unsupported	Unsupported
	Account	Dead Account Cleaner > Plan Mode	Unsupported	Unsupported
		Dead Account Cleaner > Scan Mode	Unsupported	Unsupported
	Statistics	Job Monitor	Supported	Supported
Permission Tools	Grant	Grant Permissions	Supported	Supported
		Create Group	Supported	Supported
	Modify	Edit User Permissions	Supported	Supported
		Remove User Permissions	Supported	Supported
	Manage	Permission Levels	Supported	Supported
		Anonymous Access	Unsupported	Unsupported
	Inheritance	Stop inheriting Permissions > Break Inheritance for Selected Nodes	Supported	Supported
		Stop inheriting Permissions > Break Inheritance for Sub-nodes	Supported	Supported
		Inherit Permissions > Apply Inheritance to Selected Node	Supported	Supported
		Inherit Permissions > Push Inheritance to Sub-nodes	Supported	Supported
Users and Permissions	People and Groups	All people > Delete User from Site Collection	Supported	Supported
		Group > New Group	Supported	Supported
		Group > Edit Group Setting	Supported	Supported
		Add Users	Supported	Supported
		Remove User from Group	Supported	Supported
		Group settings	Supported	Supported
Policy Enforcer	All groups	All functions	Supported	Supported

List/Library Level Operations

Refer to the table below for information about supported and unsupported functions at the list/library level.

*Note: Some cells in the tables below indicate partial support. For details on unsupported options, refer to Unsupported Options for Office 365 and Remote Farms.

Tab	Group	Function	SharePoint 2010 Online	SharePoint 2013 Online
Management	Contribute	New Folder	Supported	Supported

Tab	Group	Function	SharePoint 2010 Online	SharePoint 2013 Online
		Delete	Supported	Supported
		Admin Search > Admin Search Wizard Mode	Supported	Supported
		Admin Search > Admin Search Form Mode	Supported	Supported
		Admin Search > Start with a Predefined Search	Supported	Supported
	General Management	No Checked In Version Files	Supported	Supported
		Workflow Settings	Supported	Supported
		Metadata and Keywords Settings	Supported	Supported
		Information Management Policy Settings	Unsupported	Unsupported
	Columns	Indexed Columns	Supported	Supported
	Statistics	Job Monitor	Supported	Supported
Configuration	General Management	Versioning Settings	Supported	Supported
		Advanced Settings	Supported	Supported
		Validation Settings	Supported	Supported
		General Settings > Column Default Value Settings	Unsupported	Unsupported
		General Settings > Rating Settings	Supported	Supported
		General Settings > Audience Targeting Settings	Supported	Supported
		General Settings > Metadata Navigation Settings	Supported	Supported
		General Settings > Pre-location View Settings	Supported	Supported
		General Settings > RSS Setting	Supported	Supported
	Look and Feel	Title, Description and Navigation	Supported	Supported
Security	Contribute	List/Library Permissions	Supported	Supported
		Security Search > Security Search Wizard Mode	Supported	Supported
		Security Search > Security Search Form Mode	Supported	Supported
		Security Search > Start with a Predefined Search	Supported	Supported
	Permission	Clone Permission > Clone User Permissions	Unsupported	Unsupported

Tab	Group	Function	SharePoint 2010 Online	SharePoint 2013 Online
		Clone Permission > Clone List/Library Permissions	Unsupported	Unsupported
		Grant Permissions	Supported	Supported
		Stop inheriting Permissions > Break Inheritance for Selected Nodes	Supported	Supported
		Stop inheriting Permissions > Break Inheritance for Sub-nodes	Supported	Supported
		Inherit Permissions > Apply Inheritance to Selected Nodes	Supported	Supported
		Inherit Permissions > Push Inheritance to Sub-nodes	Supported	Supported
		Anonymous Access	Unsupported	Unsupported
	Share and Track	Alert me > Set Alert on this List/Library	Unsupported	Unsupported
		Alert me > Manage My Alert	Unsupported	Unsupported
Permission Tools	Inheritance	Stop inheriting Permissions > Break Inheritance for Selected Nodes	Supported	Supported
		Stop inheriting Permissions > Break Inheritance for Sub-nodes	Supported	Supported
		Inherit Permissions > Apply Inheritance to Selected Nodes	Supported	Supported
		Inherit Permissions > Push Inheritance to Sub-nodes	Supported	Supported
	Grant	Grant Permissions	Supported	Supported
	Modify	Edit User Permissions	Supported	Supported
		Remove User Permissions	Supported	Supported
	Manage	Anonymous Access	Unsupported	Unsupported

Folder Level Operation

Refer to the table below for the information about the supported and unsupported functions at the folder level.

*Note: Some cells in the tables below indicate partial support. For details on unsupported options, refer to [Unsupported Options for Office 365 and Remote Farms](#).

Tab	Group	Function	SharePoint 2010 Online	SharePoint 2013 Online
Management	Contribute	New Folder	Supported	Supported
		Admin Search > Admin Search Wizard Mode	Supported	Supported
		Admin Search > Admin Search Form Mode	Supported	Supported
		Admin Search > Start with a Predefined Search	Supported	Supported
		Delete	Supported	Supported
		View Properties	Supported	Supported
		View Properties > Edit Properties	Unsupported	Unsupported
	Statistics	Job Monitor	Supported	Supported
Security	Contribute	Folder Permissions	Supported	Supported
		Security Search > Security Search Wizard Mode	Supported	Supported
		Security Search > Security Search Form Mode	Supported	Supported
		Security Search > Start with a Predefined Search	Supported	Supported
	Permission	Clone Permission > Clone User Permissions	Supported	Supported
		Clone Permission > Clone Folder Permissions	Unsupported	Unsupported
		Grant Permissions	Supported	Supported
		Stop inheriting Permissions > Break Inheritance for Selected Nodes	Supported	Supported
		Stop inheriting Permissions > Break Inheritance for Sub-nodes	Supported	Supported
		Inherit Permissions > Apply Inheritance to Selected Nodes	Supported	Supported
		Inherit Permissions > Push Inheritance to Sub-nodes	Supported	Supported
	Alert	Alert Me	Unsupported	Unsupported

Tab	Group	Function	SharePoint 2010 Online	SharePoint 2013 Online
	Statistics	Job Monitor	Supported	Supported
Permission Tools	Grant	Grant Permissions	Supported	Supported
	Modify	Edit User Permissions	Supported	Supported
		Remove User Permissions	Supported	Supported
	Inheritance	Stop inheriting Permissions > Break Inheritance for Selected Nodes	Supported	Supported
		Stop inheriting Permissions > Break Inheritance for Sub-nodes	Supported	Supported
		Inherit Permissions > Apply Inheritance to Selected Nodes	Supported	Supported
		Inherit Permissions > Push Inheritance to Sub-nodes	Supported	Supported

Item Level Operation

Refer to the table below for the information about the supported and unsupported functions at the item level.

Note: Some cells in the tables below indicate partial support. For details on unsupported options, refer to Unsupported Functionalities for Office 365 or Remote Farms.

Tab	Group	Function	SharePoint 2010 Online	SharePoint 2013 Online
Management	Contribute	Admin Search > Admin Search Wizard Mode	Supported	Supported
		Admin Search > Admin Search Form Mode	Supported	Supported
		Admin Search > Start with a Predefined Search	Supported	Supported
		Delete	Supported	Supported
	Action	Change Metadata	Supported	Supported
	Statistics	Job Monitor	Supported	Supported
Security	Contribute	Item Permissions	Supported	Supported
		Security Search > Security Search Wizard Mode	Supported	Supported
		Security Search > Security Search Form Mode	Supported	Supported
		Security Search > Start with a Predefined Search	Supported	Supported

Tab	Group	Function	SharePoint 2010 Online	SharePoint 2013 Online
	Permission	Grant Permissions	Supported	Supported
		Stop inheriting Permissions > Break Inheritance for Selected Node	Supported	Supported
		Inherit Permissions > Apply Inheritance to Selected Node	Supported	Supported
	Alert	Alert Me	Unsupported	Unsupported
	Statistics	Job Monitor	Supported	Supported
Permission Tools	Inheritance	Stop inheriting Permissions > Break Inheritance for Selected Node	Supported	Supported
		Inherit Permissions > Apply Inheritance to Selected Node	Supported	Supported
	Grant	Grant Permissions	Supported	Supported
	Modify	Edit User Permissions	Supported	Supported
		Remove User Permissions	Supported	Supported

Item Version Level Operation

Refer to the table below for the information about the supported and unsupported functions at the item version level.

Note: Some cells in the tables below indicate partial support. For details on unsupported options, refer to Unsupported Functionalities for Office 365 or Remote Farms.

Tab	Group	Function	SharePoint 2010 Online	SharePoint 2013 Online
Management	Contribute	Delete	Supported	Supported
	Statistics	Job Monitor	Supported	Supported

Security Search Results Operation

Refer to the table below for the information about the supported and unsupported functions when using the Security Search Results.

Note: Some cells in the tables below indicate partial support. For details on unsupported options, refer to Unsupported Functionalities for Office 365 or Remote Farms.

View Type	Tab	Group	Function	SharePoint 2010 Online	SharePoint 2013 Online
Tree View	(Group) Tools	Contribute	Create Group	Supported	Supported
			Add Users	Supported	Supported
			Group Settings	Supported	Supported
			Edit Group Permissions	Supported	Supported
			Remove Group Permissions	Supported	Supported
			Clone User Permission	Unsupported	Unsupported
			Dead Account Cleaner	Unsupported	Unsupported
		Export and Import	Download Report	Supported	Supported
			Export for Editing	Supported	Supported
			Import Configuration File	Unsupported	Unsupported
	(User) Tools	Contribute	Grant Permissions	Supported	Supported
			Edit User Permissions	Supported	Supported
			Remove User Permissions	Supported	Supported
			Delete Users	Supported	Supported
			Clone User Permission	Unsupported	Unsupported
			Dead Account Cleaner	Unsupported	Unsupported
		Export and Import	Download Report	Supported	Supported
			Export for Editing	Supported	Supported
			Import Configuration File	Unsupported	Unsupported
	Users in Group	Contribute	Remove Users From Group	Supported	Supported
			Change Group	Supported	Supported
			Delete Users	Supported	Supported
			Clone User Permission	Unsupported	Unsupported
			Dead Account Cleaner	Unsupported	Unsupported
		Export and Import	Download Report	Supported	Supported
			Export for Editing	Supported	Supported
			Import Configuration File	Unsupported	Unsupported
	Site Administrator	Contribute	Site Collection Administrator	Supported	Supported
			Primary and Secondary Administrator	Unsupported	Unsupported
		Export and Import	Download Report	Supported	Supported
			Export for Editing	Supported	Supported
			Import Configuration File	Unsupported	Unsupported
List View	Users in Group	Contribute	Remove Users From Group	Supported	Supported
			Change Group	Supported	Supported

View Type	Tab	Group	Function	SharePoint 2010 Online	SharePoint 2013 Online
			Delete Users	Supported	Supported
			Clone User Permission	Unsupported	Unsupported
			Dead Account Cleaner	Unsupported	Unsupported
		Export and Import	Download Report	Supported	Supported
			Export for Editing	Supported	Supported
			Import Configuration File	Unsupported	Unsupported
	Users	Contribute	Edit User Permissions	Supported	Supported
			Remove User Permissions	Supported	Supported
			Delete Users	Supported	Supported
			Clone User Permission	Unsupported	Unsupported
			Dead Account Cleaner	Unsupported	Unsupported
		Export and Import	Download Report	Supported	Supported
			Export for Editing	Supported	Supported
			Import Configuration File	Unsupported	Unsupported
	Groups	Contribute	Add Users	Supported	Supported
			Group Settings	Supported	Supported
			Edit Group Permissions	Supported	Supported
			Remove Group Permissions	Supported	Supported
			Clone User Permission	Unsupported	Unsupported
			Dead Account Cleaner	Unsupported	Unsupported
		Export and Import	Download Report	Supported	Supported
			Export for Editing	Supported	Supported
			Import Configuration File	Unsupported	Unsupported
	Site Administrator	Contribute	Site Collection Administrator	Supported	Supported
			Primary and Secondary Administrator	Unsupported	Unsupported
		Export and Import	Download Report	Supported	Supported
			Export for Editing	Supported	Supported
			Import Configuration File	Unsupported	Unsupported

Unsupported Functionalities for Office 365 or Remote Farms

Unsupported Options for Office 365 and Remote Farms

The table below details options not supported for Office 365 sites or remote farms.

Feature	Unsupported
Security Search	- Search for deactivated users - Include Active Directory group members or Form-based Authentication role members - Include SharePoint users and groups with no permissions
Clone User Permission	- User Alert Properties - Change Metadata

Unsupported Admin and Security Search Filters for Office 365 or Remote Farms

The table below contains detailed information on the unsupported filters when performing Admin or Security searches on Office 365 sites or remote farms.

Level	Unsupported
Site Collection	- Template Rule - Size rule - Audit Rule - Anonymous Access Rule - Custom Properties Rule

Level	Unsupported
Site	- Template Rule - Owner Rule - Created By Rule - Auditing Rule - Anonymous Access Rule - Custom Properties Rule
List	- Created By Rule - Auditing Rule - Anonymous Access Rule
Folder	Auditing Rule

Appendix G: Supported List of Policy Enforcer Rules for SharePoint On-premises and SharePoint Online

Refer to the table below for the supported and unsupported Policy Enforcer rules for SharePoint On-premises farms and SharePoint Online site collections.

Rule	SharePoint On-premises	SharePoint Online
Site Creation	Supported	Unsupported
List or Library Creation	Supported	Unsupported
Site Template	Supported	Supported
Content Creation/Content Upload	Supported	Supported
Site Depth	Supported	Supported
Grant, Revoke and/or Modify Permissions Privilege	Supported	Supported
Permission Modification Protection	Supported	Supported
Break Inheritance Protection	Supported	Supported
Delete	Supported	Supported
Move	Supported	Supported
Copy	Supported	Supported
Microfeed Permissions Enforcement	Supported	Supported
Farm Feature	Supported	Unsupported
Web Application Feature	Supported	Unsupported
Recycle Bin	Supported	Unsupported
Site Collection Feature	Supported	Supported
Site Feature	Supported	Supported
Site Collection Navigation	Supported	Supported
Site Collection Lock	Supported	Unsupported
Property Bag	Supported	Supported
Site Theme	Supported	Supported
Master Page	Supported	Supported
List Versioning Settings	Supported	Supported
Library Versioning Settings	Supported	Supported
Information Rights Management (IRM) SharePoint 2010	Supported	Supported
Information Rights Management (IRM) SharePoint 2013	Supported	Supported
Active Directory Group Depth	Supported	Unsupported
Site Size	Supported	Unsupported
Restricted Subsite Template	Supported	Supported
Site Collection Administrators Count	Supported	Supported
Site Content Type Deployment	Supported	Unsupported
List Content Type Deployment	Supported	Unsupported
Site Column Type Deployment	Supported	Unsupported
List Column Type Deployment	Supported	Unsupported

Web Part Mandatory Block	Supported	Unsupported
Search and Offline availability	Supported	Unsupported
User/Group Restriction	Supported	Unsupported

DocAve 6: Administrator

Notices and Copyright Information

Notice
The materials contained in this publication are owned or provided by AvePoint, Inc. and are the property of AvePoint or its licensors, and are protected by copyright, trademark and other intellectual property laws. No trademark or copyright notice in this publication may be removed or altered in any way.

Copyright
Copyright © 2012-2014 AvePoint, Inc. All rights reserved. All materials contained in this publication are protected by United States and international copyright laws and no part of this publication may be reproduced, modified, displayed, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of AvePoint, 3 Second Street, Jersey City, NJ 07311, USA or, in the case of materials in this publication owned by third parties, without such third party's consent. Notwithstanding the foregoing, to the extent any AvePoint material in this publication is reproduced or modified in any way (including derivative works and transformative works), by you or on your behalf, then such reproduced or modified materials shall be automatically assigned to AvePoint without any further act and you agree on behalf of yourself and your successors, assigns, heirs, beneficiaries, and executors, to promptly do all things and sign all documents to confirm the transfer of such reproduced or modified materials to AvePoint.

Trademarks
AvePoint®, DocAve®, the AvePoint logo, and the AvePoint Pyramid logo are registered trademarks of AvePoint, Inc. with the United States Patent and Trademark Office. These registered trademarks, along with all other trademarks of AvePoint used in this publication are the exclusive property of AvePoint and may not be used without prior written consent.

Microsoft, MS-DOS, Internet Explorer, Microsoft Office SharePoint Servers 2007/2010, SharePoint Portal Server 2003, Windows SharePoint Services, Windows SQL server, and Windows are either registered trademarks or trademarks of Microsoft Corporation.

Adobe Acrobat and Acrobat Reader are trademarks of Adobe Systems, Inc.

All other trademarks contained in this publication are the property of their respective owners and may not be used without such party's consent.

Changes
The material in this publication is for information purposes only and is subject to change without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, AvePoint makes no representation or warranty, expressed or implied, as to its completeness, accuracy, or suitability, and assumes no liability resulting from errors or omissions in this publication or from the use of the information contained herein. AvePoint reserves the right to make changes in the Graphical User Interface of the AvePoint software without reservation and without notification to its users.

AvePoint, Inc.
Harborside Financial Center, Plaza 10
3 Second Street, 9th Floor
Jersey City, New Jersey 07311
USA