



DocAve® 6.0.1 Administrator

User Guide

Revision B
Issued April 2012

Table of Contents

Table of Contents.....	2
About DocAve Administrator for SharePoint.....	5
Complementary Products.....	5
Submitting Documentation Feedback to AvePoint	5
Before You Begin.....	6
Configuration	6
Agents	6
Licensing and Permissions	6
Local System Permissions	7
Getting Started.....	8
Launching Administrator for SharePoint	8
User Interface Overview	9
Selecting Farms and Nodes.....	10
Viewing and Searching Content.....	11
Viewing Site Collection Lists.....	11
Viewing Users and Permissions	11
Performing an Admin Search using Admin Search Wizard	12
Performing an Admin Search using Admin Search Form Mode	13
Performing a Security Search using Security Search Wizard	13
Performing a Security Search using Security Search Form Mode.....	15
Using a Predefined Search	15
Managing Content	16
Creating Site Collections and Content Databases.....	16
Deploying Site Maximum Depth	16
Extending Web Applications.....	17
Moving Site Collections across Content Databases.....	17
Checking for Broken Links.....	18
Searching Web Parts	19
Search Web Parts.....	19

Further Operations for Search Web Parts in Job Monitor	20
Searching Alerts	20
Deleting Web Applications.....	21
Deleting Orphan Sites	21
Scanning on the Back-end and Saving as a Plan	22
Scanning Immediately on the Front-end	23
Additional Operations for Deleting Orphan Sites in Job Monitor.....	24
Right-Click Operations for Each Level	24
Managing Security	26
Cloning User Permissions.....	26
Cloning Site Permissions	27
Using Dead Account Cleaner.....	28
Using Plan Mode	28
Using Scan Mode.....	29
Additional Operations for Dead Account Cleaner in Job Monitor	30
Importing a Configuration File	31
Exporting, Editing, and Importing Configuration Files.....	31
Exporting the Configuration File	31
Modifying an Exported Configuration File	31
Importing the Configuration File.....	32
Downloading Search Reports.....	32
DocAve Administrator for SharePoint Use Cases	33
Security Permissions Search	33
Employee Shuffling and Permissions Cloning	34
Solution to a Database Becoming Too Large	35
Appendix A.....	36
Search Filter Table.....	36
Appendix B	48
DocAve Administrator and SharePoint Operations	48
Farm Level Operations	48
Web Application Level Operations	51
Site Collection Level Operations	53

Sub-site Level Operations	56
List/Library Level Operations	59
Folder Level Operations	61
Item Level Operations.....	63
Appendix C	64
Security Search Result.....	64
Index.....	66
Notices and Copyright Information	67

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 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. Click the following URL to access the **Submit Your Feedback** form on our Web site:

<http://www.avepoint.com/resources/documentation-feedback/?flush=1>

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.

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. At the minimum, DocAve must have one agent installed on the SharePoint farm. The server that the agent is installed on must have Microsoft SharePoint Foundation Web Application service enabled as well. Otherwise, the Administrator Agent cannot be loaded during agent installation and, consequently, the Administrator functions cannot be used. Additional DocAve agents should be installed on other SharePoint Web front ends (WFEs) in order to provide redundancy in the event that a DocAve Agent goes down.

***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](#).

Licensing and Permissions

To install and use Administrator for SharePoint 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.
3. 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.

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, follow the instructions below:

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 **Central Admin** to launch Administrator for SharePoint.

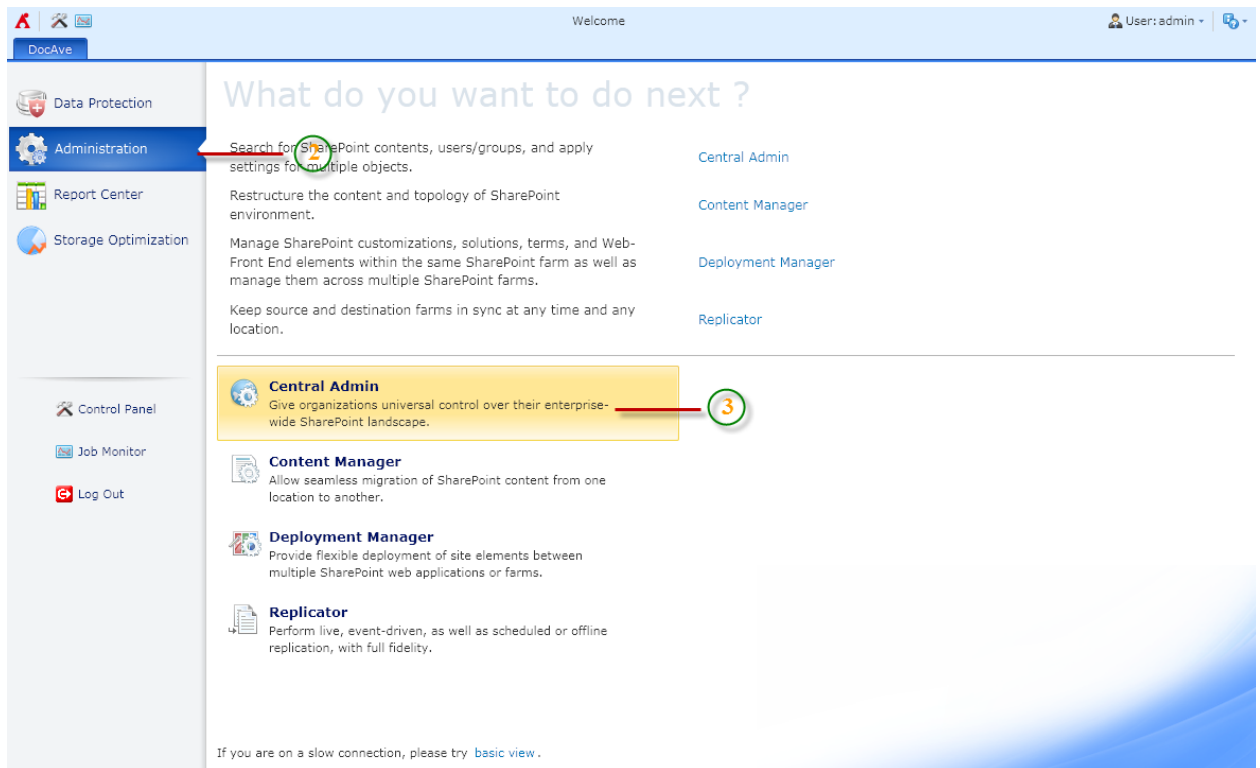


Figure 1: DocAve module launch window.

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.

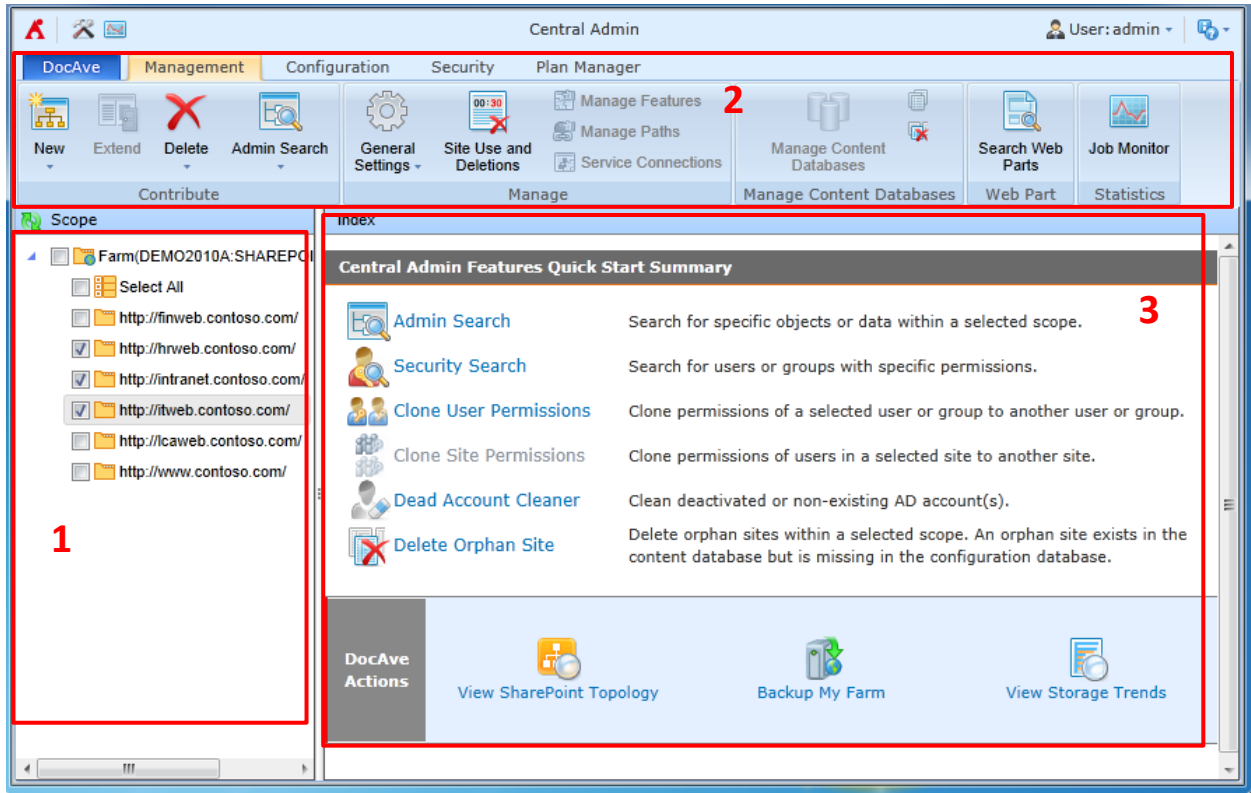


Figure 2: Administrator (Central Admin) user interface.

1. The **SharePoint tree (Scope panel)** displays all content within your farm(s). 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:

1. From the **Scope** panel on the left, double-click the farm that contains the relevant SharePoint content.
2. Select the relevant content from which you want to perform further operations by clicking the checkbox(es) to the left of the content.
3. After selecting content, you will be able to perform the procedures described throughout this guide.

***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 collection(s) on the tree for which the user is a site collection administrator. 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 level. For details about how to configure the Security Trimming, refer to the [DocAve 6 Control Panel Reference Guide](#).

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 node, follow the instructions below. Note that you can only view site collection lists for one node 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**.

This functionality also exists within SharePoint. 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 [DocAve Administrator and SharePoint Operations](#) in **Appendix B**.

Viewing Users and Permissions

To view a list of user permissions for people and groups or a list of site permissions:

1. Select the **Scope** of the content, as described in [Selecting Farms and Nodes](#).
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. 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 [DocAve Administrator and SharePoint Operations](#) in **Appendix B**.

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. To perform an admin search using the Wizard:

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. Add an optional **Description** if desired.
4. Click **Next** on the ribbon. The **Search Filter** screen appears.
5. 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 the [Search Filter Table](#) in **Appendix A**.
 - Change the logical relationship between two or more filter rules by clicking **And** or **Or** to the right of the list entry.
 - **And** – The content that meets all the rules is displayed.
 - **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.
6. When finished setting up filter rules, click **Next** on the ribbon. The **Schedule Selection** screen appears.
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** on the ribbon. The **Notification** screen appears.
9. Using the drop-down boxes, select the type of report (**Summary** or **Detailed**), enter the recipient's e-mail address, and click **Add**. Repeat this procedure for any additional recipients.
10. When finished setting up notifications, click **Next** on the ribbon. The **Overview** screen appears.
11. 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.
12. 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 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**. This search is configured with no sequence. For detailed information about how to configure an admin search condition, refer to [Performing Admin Searches 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:

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. 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.
6. Click **Advanced** to specify the relevant search conditions.
 - **Search for deactivated users** – Check 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 group members** – Check 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.

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. Enter 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 **Full Control, Design, 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.
 - **Only search explicit permissions** – Only search the SharePoint objects with explicit permission in selected node(s).
8. When finished, click **Next** on the ribbon. The **Search Filter** screen appears.
9. 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 the [Search Filter Table](#) in **Appendix A**.
 - Change the logical relationship between two or more filter rules by clicking **And** or **Or** to the right of the list entry.
 - **And** – The content that meets all the rules is displayed.
 - **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.
10. When 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. Using the drop-down boxes, select the type of report (**Summary** or **Detailed**), enter the recipient's e-mail address, and click **Add**. Repeat this procedure for any additional recipients.

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](#) 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**. This search is configured with no sequence. For detailed information about how to configure a security search condition, refer to [Performing Security Searches 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](#) 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:

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:

1. Select the farm or node to create a new site collection 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. 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 [DocAve Administrator and SharePoint Operations](#) in **Appendix B**.

Deploying Site Maximum Depth

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

To deploy a site maximum depth:

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 websites 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:

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. 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 [DocAve Administrator and SharePoint Operations](#) in **Appendix B**.

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:

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 site(s) offline. When performing this operation, DocAve locks the site(s) as **Read-only**.

- **Notification** – Configure email notification settings. Using the drop-down boxes, select the type of report (**Summary** or **Detailed**), enter the recipient’s e-mail address, and click **Add**. Repeat this procedure for any additional recipients.
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:

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. 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.
 - **External links depth limit** – Input a positive number to limit the internal links depth.

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** – Check all the links’ URLs.
 - **Include URLs that match the criteria** – Input the full URL of the link (s) that you wish to check during the scan.
 - **Exclude the URLs that match the criteria** – Input the full URL of the link(s) that you wish to ignore during the scan.
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. Using the drop-down boxes, select the type of report (**Summary** or **Detailed**), enter the recipient's e-mail address, and click **Add**. Repeat this procedure for any additional recipients.
 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

Follow the instructions below to search web parts.

1. Click **Management** tab > **Search Web Parts**. The **Search Web Parts** page appears.
2. Enter a **Plan Name**, and 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 <i>len</i> is displayed.
	Is(exactly)	Announcements	The web part whose title is <i>Announcements</i> is displayed.
Template Name	Contains	DataAssociation	The web part whose template name contains <i>DataAssociation</i> is displayed.
	Is(exactly)	AuthoredListFilter.webpart	The web part whose template name is <i>AuthoredListFilter</i> is displayed.
Page URL	Contains	AnalyticsReports	The web part whose page URL contains <i>AnalyticsReports</i> is displayed.
	Is(exactly)	http://test:2000/ReportsList/AllItems.aspx	The web part whose page URL is <i>http://test:2000/ReportsList/AllItems.aspx</i> 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. Configure email **Notification** settings. Using the drop-down boxes, select the type of report (**Summary** or **Detailed**), enter the recipient's e-mail address, and click **Add**. Repeat this procedure for any additional recipients.
 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.

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.

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**. In **Search Alerts**, the user is guided through the following steps:

1. Select the **Users** whose alerts you want to search. Select **Display alerts for** and enter the user(s) whose alerts you wish to search. Click the **Check Names** icon to verify the inputted names, or click the **Browse** icon to browse through the names.
2. Select the lists/libraries (**Scope**) 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:

1. Select the site collection 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. 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 [DocAve Administrator and SharePoint Operations](#) in **Appendix B**.

Deleting Orphan Sites

An orphan site can be thought of as a site or sub-site that no longer has a content owner. This situation may come about, for example, when a person leaves an organization. The content within that person's site(s) remains on the server, using up valuable server space.

A second meaning for an orphaned site has to do with a site collection's URL path being inaccessible. This can happen when trying to attach a content database to a web application. If in that content database there's information about a site collection with a specific URL, but in the web application there's already a site collection using the same path, the site collection being attached will be inaccessible.

In either of these situations, it may be desirable to delete the orphan sites using the **Delete Orphan Sites** feature. There are two modes that can be used for deleting an orphan site: **Scan on the back-end and save as a plan**, and **Scan now on the front-end**. A front-end action is one in which the user waits for a system response or report before any further actions can be performed. Back-end actions are actions performed in the background of DocAve, enabling the user to continue navigating through the user interface without worrying about prematurely ending the action.

To remove orphan sites:

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 **Scan on the back-end and save as a plan**, or **Scan now on the front-end**. Proceed to the section below that is appropriate to your selection.




Scanning on the Back-end and Saving as a Plan

Back-end scans generally take 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. Proceed with the procedure below if you'd like to **Scan on the back-end and save as a plan**:

1. Enter a **Plan Name** for the plan. 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. Using the drop-down boxes, select the type of **Email Notification** report (Summary or Detailed), enter the recipient's e-mail address, and click **Add**. Repeat this procedure for any additional recipients.
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 Immediately on the Front-end

Front-end scans are completed faster than back-end scans; however, navigating away from the current user interface screen will terminate the scan. Proceed with the procedure below if you'd like to **Scan immediately on the front-end**:

1. After selecting **Scan now on the front-end**, 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 site(s) 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. Using the drop-down boxes, select the type of **Email Notification** report (**Summary** or **Detailed**), enter the recipient's e-mail address, and click **Add**. Repeat this procedure for any additional recipients.
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.

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 site(s) that you want to delete.
3. Click **Next** to configure the schedule and notification. For details on these configurations, refer to [Scanning Immediately on the Front-end](#).
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.

Right-Click Operations for 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
	Manage Permission Policy Levels	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	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.

Cloning User Permissions

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

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 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 name to the destination name.
 - **Replace** – Replaces the destination permission with the source permission.
6. Select the **Permission Rule**. This determines how DocAve Administrator will handle the permissions of user(s) in SharePoint group(s).
 - **Include permission inherited from groups** – Copies the permission of the group where the source user exists to destination user.
 - **Add user to the same groups in the destination** – Adds the destination user to the group where source user exists.

Example:

Assume that *user1* is a dead account that exists in SharePoint *group1*, and *user2* is *user1*'s destination user. If **Include permission inherited from groups** is selected, *group1*'s permission is cloned to *user2*. If **Include permission inherited from groups** and **Add user to the same groups in the destination** are both selected, *user2* is added into *group1*. If both **Include permission inherited from groups** and **Add user to the same groups in the destination** are not selected, *group1*'s permissions cannot be cloned to *user2*.

- **Remove source user's explicit permissions or group 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.
7. Select whether or not to turn on **User Alert Properties**. If **Yes** is selected, this copies the user alert(s) settings set by the source user to the destination user(s).
 8. Choose whether or not to **Change Metadata**. If **Yes** is selected, this transfers the corresponding source user's metadata to destination user(s). Enter the metadata column name and click **Add** to add it.
 9. 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.
 10. Using the drop-down boxes, select the type of **Email Notification** report (Summary or Detailed), enter the recipient's e-mail address, and click **Add**. Repeat this procedure for any additional recipients.
 11. When satisfied with your selections, click **OK** to start the job. Access Job Monitor to view job details.

Cloning Site Permissions

The Clone Site Permissions feature allows you to copy source user(s)/group(s) and permissions to one or more destination sites. To clone the site permissions:

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 site(s) by checking the corresponding checkbox.
4. Expand the **Farm** tree to select the **Destination Site(s)** 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. Using the drop-down boxes, select the type of **Email Notification** report (Summary or Detailed), enter the recipient’s e-mail address, and click **Add**. Repeat this procedure for any additional recipients.
 8. When satisfied with your selections, click **OK** to start the job. Access Job Monitor to view job details.

Using Dead Account Cleaner

Dead Account Cleaner allows you to remove the 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.

Using Plan Mode




To use the Plan Mode in Dead Account Cleaner:

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. Add an optional **Description** if desired.
4. 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.
5. The **Actions for My Site** option chooses how to manage “My Sites” dead accounts.
 - **Keep My Site** – Keeps My Sites of relevant dead accounts.
 - **Delete My Site** – Deletes My Sites of relevant dead accounts.
6. 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.

7. 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.
8. Using the drop-down boxes, select the type of **Email Notification** report (Summary or Detailed), enter the recipient's e-mail address, and click **Add**. Repeat this procedure for any additional recipients.
9. 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.

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 > 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 account(s) 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 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  icon, 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 alert(s) settings set by the source user to the destination user(s).
 10. Choose whether or not to **Change Metadata**. If **Yes** is selected, this transfers the corresponding source user's metadata to destination user(s). 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 user(s) in SharePoint group(s).
 - **Include permission inherited from groups** – Copies the permission of the group where the source user exists to destination user.
 - **Add user to the same groups in the destination** – Adds the destination user to the group where source user exists.
- Example:**
Assume that *user1* is a dead account that exists in SharePoint *group1*, and *user2* is *user1*'s destination user. If **Include permission inherited from groups** is selected, *group1*'s permission are cloned to *user2*. If **Include permission inherited from groups** and **Add user to the same groups in the destination** are both selected, *user2* is added into *group1*. If both **Include permission inherited from groups** and **Add user to the same groups in the destination** are not selected, *group1*'s permissions cannot be 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 orphan site operations are available in Job Monitor.

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 account(s) 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.

Importing a Configuration File

To import and apply a pre-defined configuration file into the entire farm, select the farm to which you want to apply the configuration file from the Scope panel. Click **Security > Import Configuration File**. The **Import Configuration File** page appears. Refer to the steps below:

1. Select a configuration **File Type** from the drop-down box. **Edit User Permission** imports the file generated by security search, while **Edit Group** imports the file downloaded by **Export Group for Editing**.
2. Click **Browse** to select the **Configuration File** you want to import.
3. Choose whether or not to use a **Schedule**. If you decide to configure the schedule yourself, input a start time.
4. Configure email **Notification** settings. Using the drop-down boxes, select the type of report (**Summary** or **Detailed**), enter the recipient's e-mail address, and click **Add**. Repeat this procedure for any additional recipients.
5. Click **Run** to start this job, or click **Cancel** to quit this operation. Click **Test Run** to run a test job first.

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.

See the topics below.

Exporting the Configuration File

To export the configuration file for editing:

1. Perform a security search, as described in [Viewing and Searching Content](#).
2. Access Job Monitor. When the search completes, select the job and click **Search Results**. The **Search Result Tools** tab becomes enabled.
3. Click **Export for Editing**. Save the file to a local drive.

Modifying an Exported Configuration File

To modify an exported configuration file:

1. Navigate to the location on your local drive where the exported configuration file is saved. To export a configuration file, see [Exporting the Configuration File](#).
2. Unzip the report folder.
3. Open the configuration file to update the permissions.

4. Choose to **Add**, **Delete**, or **Modify** 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 **Name** and **Permission** columns can be modified in the configuration file.

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

Importing the Configuration File

To import a configuration file back into SharePoint:

1. After editing the configuration file (as described in [Modifying an Exported Configuration File](#)), access Job Monitor.
2. Select the job and click **Search Result**. The **Search Result Tools** tab becomes enabled.
3. Click **Import Configuration File** and select from the following options.
 - **File Type** – Select a configuration file type from the drop-down box. **Edit User Permission** imports the file generated by security search, while **Edit Group** imports the file downloaded by **Export Group for Editing**.
 - **Farm Selection** – Select a farm from the drop-down box; the configuration file is applied to this farm.
 - **Configuration File** – Click **Browse** to select the configuration file to import.
4. Click **Run** to start this job, or click **Cancel** to quit this operation. Click **Test Run** to run a test job first.

Downloading Search Reports

1. Perform a security search, and access Job Monitor. After the search completes, select the job and click **Search Results**.
2. The **Tools** tab becomes enabled.
3. Click **Download Report** to download a job report.
 - **Report Format** – Select a report type from corresponding drop-down box.
4. Click **OK** to download the report.

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 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 sub-site 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 in Form Mode](#) on the HR site collection, accesses Job Monitor when the search completes, and [exports a CSV report](#) 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 [Clone 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](#). 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 his 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 new content database](#). 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 half of the site collections](#) from the nearly-full content database to the content database he just created. Joe [selects the site collections](#) to move 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 [check 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 [Delete Orphan Site](#) 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

Level	Rule	Condition	Value	Result
Web Application	URL	Contains	tes	The web application whose URL contains <i>tes</i> is searched. Search result example: <i>http://tes:30000/</i> and <i>http://test:20000/</i>
		Is(exactly)	<i>http://test:20000/</i>	The web application whose URL is <i>http://test:20000/</i> is searched.
		Match	<i>http://tes*000/</i>	The web application whose URL begins with <i>http://tes</i> and ends with <i>000/</i> is searched. Search result example: <i>http://test:20000/</i>
			<i>http://te?t:20000/</i>	The web application whose URL is the same as <i>http://te?t:20000/</i> except character <i>?</i> . Search result example: <i>http://test:20000/</i> and <i>http://text:20000/</i>
Site Collection	URL	Contains	sitecollection	The site collection whose URL contains <i>sitecollection</i> is searched. Search result example: <i>http://test:20000/sites/sitecollectionA</i> and <i>http://test:20000/sites/sitecollectionB</i>
		Is(exactly)	<i>http://test:20000/sites/sitecollectionA</i>	The site collection whose URL is <i>http://test:20000/sites/sitecollectionA</i> is searched.
		Match	<i>http://tes*collectionA</i>	The site collection whose URL begins with <i>http://tes</i> and ends with <i>collectionA</i> is searched. Search result example: <i>http://tesABC:11111/sitecollectionA</i>

			http://test:20000/sites/sitecollecti?nA	The site collection whose URL is the same as <i>http://test:20000/sites/sitecollecti?nA</i> except character <i>?</i> is searched. Search result example: <i>http://test:20000/sites/sitecollectionA</i> and <i>http://text:20000/sites/sitecollectiBnA</i>
Site Collection Title	Contains	title		The site collection whose title contains <i>title</i> is searched. Search result example: <i>titleA</i> and <i>title1</i>
	Is(exactly)	title1		The site collection whose tile is <i>title1</i> is searched.
	Match	ti*1		The site collection whose title begins with <i>ti</i> and ends with <i>1</i> is searched. Search result example: <i>title1</i>
		tit?e1		The site collection whose title is the same as <i>tit?e1</i> except character <i>?</i> is searched. Search result example: <i>titAe1</i>
Modified Time	From...To...	2011-11-11 12:15:50 2011-12-25 17:35:54		The site collection that is modified between <i>12:15:50 11/11/2011</i> and <i>17:35:54 12/25/2011</i> is searched.
	Before	2011-11-11 12:15:50		The site collection that is modified before <i>12:15:50 11/11/2011</i> is searched.
	After	2011-11-11 12:15:50		The site collection that is modified after <i>12:15:50 11/11/2011</i> is searched.
	On	2011-11-11 12:15:50		The site collection that is modified on <i>12:15:50 11/11/2011</i> is searched.
	Within days/weeks/months/years	5 Days		The site collection 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 collection that is created between <i>12:15:50 11/11/2011</i> and <i>17:35:54 12/25/2011</i> is searched.
	Before	2011-11-11 12:15:50	The site collection that is created before <i>12:15:50 11/11/2011</i> is searched.
	After	2011-11-11 12:15:50	The site collection that is created after <i>12:15:50 11/11/2011</i> is searched.
	On	2011-11-11 12:15:50	The site collection that is created on <i>12:15:50 11/11/2011</i> is searched.
	Within... days/weeks/ months/ years	5 Days	The site collection that is created in last 5 days is searched.
Primary Administrator	Contains	user	The site collection whose primary administrator's name contains <i>user</i> is searched. Search result example: <i>userA</i> and <i>user1</i>
	Is(exactly)	userA	The site collection whose primary administrator's name is <i>userA</i> is searched.
Template Name	Contains	Team	The site collection whose template name contains <i>Team</i> is searched. Search result example: <i>Team Site</i>
	Is(exactly)	Blank Site	The site collection whose template name is <i>Blank Site</i> is searched.
	Match	B*Workspace	The site collection whose template name begins with <i>B</i> and ends with <i>Workspace</i> is searched. Search result example: <i>Basic Meeting Workspace</i> and <i>Blank Meeting Workspace</i>
		Bl?g	The site collection whose template name is the same as

				<i>Bl?g</i> except character <i>?</i> is searched. Search result example: <i>Blog</i>
Site	URL	Contains	siteA	The site whose URL contains <i>siteA</i> is searched. Search result example: <i>http://test:20000/sites/site-collectionA/siteA</i> and <i>http://test:20000/sites/site-collectionA/siteAB</i>
		Is(exactly)	<i>http://test:20000/sites/sitecollectionA/siteA</i>	The site whose URL is <i>http://test:20000/sites/sitecollectionA/siteA</i> is searched.
		Match	<i>http://tes*siteA</i>	The site whose URL begins with <i>http://tes</i> and ends with <i>siteA</i> is searched. Search results example: <i>http://tesABC:11111/site-collectionA/siteA</i>
			<i>http://test:20000/sites/sitecollection?/siteA</i>	The site whose URL is the same as <i>http://test:20000/sites/site-collection?/siteA</i> except character <i>?</i> is searched. Search result example: <i>http://test:20000/sites/site-collectionA/siteA</i>
	Site Title	Contains	title	The site whose title contains <i>title</i> is searched. Search result example: <i>titleA</i> and <i>title1</i>
	Is(exactly)	title1	The site collection whose title is <i>title1</i> is searched.	
	Match	ti*1	The site whose title begins with <i>ti</i> and ends with <i>1</i> is searched. Search result example: <i>title1</i>	
		tit?e1	The site whose title is the	

				same as <i>tit?e1</i> except character <i>?</i> is searched. Search result example: <i>titAe1</i>
Modified Time	From...To...	2011-11-11 12:15:50 2011-12-25 17:35:54		The site that is modified between <i>12:15:50 11/11/2011</i> and <i>17:35:54 12/25/2011</i> is searched.
	Before	2011-11-11 12:15:50		The site that is modified before <i>12:15:50 11/11/2011</i> is searched.
	After	2011-11-11 12:15:50		The site that is modified after <i>12:15:50 11/11/2011</i> is searched.
	On	2011-11-11 12:15:50		The site that is modified on <i>12:15:50 11/11/2011</i> 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 <i>12:15:50 11/11/2011</i> and <i>17:35:54 12/25/2011</i> is searched.
	Before	2011-11-11 12:15:50		The site that is created before <i>12:15:50 11/11/2011</i> is searched.
	After	2011-11-11 12:15:50		The site that is created after <i>12:15:50 11/11/2011</i> is searched.
	On	2011-11-11 12:15:50		The site that is created on <i>12:15:50 11/11/2011</i> 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 <i>user</i> is searched. Search result example: <i>userA</i> and <i>user1</i>

		Is(exactly)	userA	The site created by the user whose name is <i>userA</i> is searched.
	Template Name	Contains	Team	The site whose template name contains <i>Team</i> is searched. Search result example: <i>Team Site</i>
		Is(exactly)	Blank Site	The site whose template name is <i>Blank Site</i> is searched.
		Match	B*Workspace	The site whose template name begins with <i>B</i> and ends with <i>Workspace</i> is searched. Search result example: <i>Basic Meeting Workspace</i> and <i>Blank Meeting Workspace</i>
			Bl?g	The site whose template name is the same as <i>Bl?g</i> except character <i>?</i> is searched. Search result example: <i>Blog</i>
	Inheritance	Is(exactly)	Inherited Permission	The site that has inherited permission from its parent node is searched.
			Explicit Permissions	The site that has explicit permission from its parent node is searched.
List/Library	URL	Contains	libraryA	The library whose URL contains <i>libraryA</i> is searched. Search result example: <i>http://test:20000/sites/sitecollectionA/siteA/LibraryA</i> and <i>http://test:20000/sites/stiecollectionA/siteA/libraryAB</i>
		Is(exactly)	<i>http://test:20000/sites/sitecollectionA/siteA/LibraryA</i>	The library whose URL is <i>http://test:20000/sites/sitecollectionA/siteA/libraryA</i>
	Name	Contains	lib	The library whose name contains <i>lib</i> will be searched

				out. For example, <i>libraryA</i> and <i>lib123</i> is searched..
		Is(exactly)	libraryA	The library whose name is <i>libraryA</i> is searched.
		Match	li*A	The library whose title begins with <i>li</i> and ends with <i>A</i> is searched. Search result example: <i>libraryA</i>
			libra?yA	The library whose title is the same as <i>librara?yA</i> except character <i>?</i> is searched. Search results example: <i>libraryA</i>
Modified Time	From...To...	2011-11-11 12:15:50 2011-12-25 17:35:54		The list/library that is modified between <i>12:15:50 11/11/2011</i> and <i>17:35:54 12/25/2011</i> is searched.
	Before	2011-11-11 12:15:50		The list/library that is modified before <i>12:15:50 11/11/2011</i> is searched.
	After	2011-11-11 12:15:50		The list/library that is modified after <i>12:15:50 11/11/2011</i> is searched.
	On	2011-11-11 12:15:50		The list/library that is modified on <i>12:15:50 11/11/2011</i> 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 <i>12:15:50 11/11/2011</i> and <i>17:35:54 12/25/2011</i> is searched.
	Before	2011-11-11 12:15:50		The list/library that is created before <i>12:15:50 11/11/2011</i> is searched.
	After	2011-11-11 12:15:50		The list/library that is created after <i>12:15:50 11/11/2011</i> is searched.
	On	2011-11-11 12:15:50		The list/library that is created on <i>12:15:50 11/11/2011</i> is

				searched.
		Within... days/weeks/ months/ years	5 Days	The list/library that is created in last 5 days is searched.
	Created By	Contains	use	The list/library created by the user whose name contains <i>use</i> is searched. Search result example: <i>userA</i>
		Is(exactly)	userA	The list/library that is created by <i>userA</i> is searched.
	Inheritance	Is(exactly)	Inherited Permission	The list/library that has inherited permission from its parent node is searched.
			Explicit Permissions	The list/library that has explicated permission from its parent node is searched.
Folder	Name	Contains	folder	The folder whose name contains <i>folder</i> is searched.
		Is(exactly)	folderA	The folder whose name is <i>folderA</i> is searched.
		Match	fol*A	The folder whose name begins with <i>fol</i> and ends with <i>A</i> is searched.
			fold?rA	The folder whose name is the same as <i>fold?rA</i> except character <i>?</i> is searched. Search results example: <i>folderA</i>
	Inheritance	Is(exactly)	Inherited Permission	The folder that has inherited permission from its parent node is searched.
			Explicit Permissions	The folder that has explicated permission from its parent node is searched.
Item	Name	Contains	item	The item whose name contains <i>item</i> is searched.
		Is(exactly)	itemA	The item whose name is <i>itemA</i> is searched.
		Match	it*A	The item whose name begins with <i>it</i> and ends with <i>is</i>

				searched. Search result example: itemA	
			ite?A	The item whose name is the same as <i>ite?A</i> except character ? is searched. Search result example: <i>itemA</i>	
	Inheritance	Is(exactly)	Inherited Permission	The item that has inherited permission from its parent node is searched.	
			Explicit Permissions	The item that has explicated permission from its parent node is searched.	
	Content Type	Is(exactly)	typeA	The item whose content type is <i>typeA</i> is searched.	
	Versions	Only Latest []	Versions	3	The item's last 3 versions are searched.
			Major Versions	3	The item's last 3 major versions are searched.
			Major Versions	N/A	All major versions are searched.
			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.	
			Is(exactly)	demo.doc	The document whose document name and extension is <i>demo.doc</i> is searched.
			Match	dem*!sc	The document whose document name and extension begins with <i>dem</i> and ends with <i>!sc</i> is searched.
				demo.x?sc	The document whose document name and extension is the same as <i>demo.x?sc</i> except character ?

				is searched.
	Inheritance	Is(exactly)	Inherited Permission	The document that has inherited permission from its parent node is searched.
			Explicit Permissions	The document that has explicated permission from its parent node is searched.
	Content Type	Is(exactly)	typeA	The item whose content type is <i>typeA</i> is searched.
	Versions	Only Latest []	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.

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	Contains	user	Full Control	Exact permission	The site collection whose user name is <i>user</i> and whose user permission is <i>Full Control</i> is searched.
			user		Exact permission or better	The site collection whose user name is <i>user</i> and whose user permission is equal or better than <i>Full Control</i> is searched.
			user	Design	Exact permission	The site collection whose user name is <i>user</i> and whose user permission is <i>Design</i> is searched.
			user		Exact permission or better	The site collection whose user name is <i>user</i> and whose user permission is equal or better than <i>Design</i> is searched.
			user	Contribute	Exact permission	The site collection whose user name is <i>user</i> and whose user permission is <i>Contribute</i> is searched.
			user		Exact permission or better	The site collection whose user name is <i>user</i> and whose user permission is <i>Contribute</i> is searched.
			user	Read	Exact permission	The site collection whose user name is <i>user</i> and whose user permission is <i>Read</i> is searched.
			user		Exact permission or better	The site collection whose user name is <i>user</i> and whose user

						permission is <i>Read</i> is searched.
			user	View Only	Exact permission	The site collection whose user name is <i>user</i> and whose user permission is <i>View Only</i> is searched.
			user		Exact permission or better	The site collection whose user name is <i>user</i> and whose user permission is <i>View Only</i> is searched.
			user	Limited Access	Exact permission	The site collection whose user name is <i>user</i> and whose user permission is <i>Limited Access</i> is searched.
			user		Exact permission or better	The site collection whose user name is <i>user</i> and whose user permission is <i>Limited Access</i> is searched.

Appendix B

DocAve Administrator and SharePoint Operations

Farm Level Operations

Operation	Location in DocAve	Location in SharePoint	Batch Settings
Management			
New	Management > Contribute	Central Administration > Application Management	Unsupported
Admin Search Wizard Mode	Management > Contribute	N/A	Unsupported
Admin Search Form Mode	Management > Contribute	N/A	Unsupported
Start with a Predefined Search	Management > Contribute	N/A	Unsupported
Manage Farm Features	Management > System Settings	Central Administration > System Settings	Unsupported
Manage Farm Solutions	Management > System Settings	Central Administration > System Settings	Unsupported
Manage User Solutions	Management > System Settings	Central Administration > System Settings	Unsupported
Servers in Farm	Management > System Settings	Central Administration > System Settings	Unsupported
Services on Server	Management > System Settings	Central Administration > System Settings	Unsupported
Quiesce Farm	Management > System Settings	To achieve by command line.	Unsupported
Manage Service Applications	Management > Application Management	Central Administration > Application Management	Unsupported
Search Service	Management > Application Management	Central Administration > Application Management	Unsupported
Default Database Server	Management > Application Management	Central Administration > Application Management	Unsupported
Data Retrieval Service	Management > Application Management	Central Administration > Application Management	Unsupported
Specify Quota Templates	Management > Application	Central Administration > Application Management	Unsupported

	Management		
Review Database Status	Management > Upgrade and Patch	Central Administration > Upgrade and Migration	Unsupported
Check Product and Patch Installation Status	Management > Upgrade and Patch	Central Administration > Upgrade and Migration	Unsupported
Job Monitor	Management > Statistics	N/A	N/A
Configuration			
Configure Outgoing E-mail Settings	Configuration > Farm Configuration	Central Administration > System Settings	Unsupported
Configure Incoming E-mail Settings	Configuration > Farm Configuration	Central Administration > System Settings	Unsupported
Configure Mobile Account	Configuration > Farm Configuration	Central Administration > System Settings	Unsupported
Alternate Access Mappings	Configuration > Farm Configuration	Central Administration > System Settings	Unsupported
Privacy Options	Configuration > Farm Configuration	Central Administration > System Settings	Unsupported
Cross-Firewall Access Zone	Configuration > Farm Configuration	Central Administration > System Settings	Unsupported
Records Center	Configuration > Farm Configuration	To achieve by command line.	Unsupported
Manage Form Templates	Configuration > General Application Settings	Central Administration > General Application Settings	Unsupported
Configure InfoPath Forms Services	Configuration > General Application Settings	Central Administration > General Application Settings	Unsupported
Upload Form Template	Configuration > General Application Settings	Central Administration > General Application Settings	Unsupported
Manage Data Connection Files	Configuration > General Application Settings	Central Administration > General Application Settings	Unsupported
Configure InfoPath Forms Services Web Service Proxy	Configuration > General Application Settings	Central Administration > General Application Settings	Unsupported
Crawler Impact Rules	Configuration > General Application	Central Administration > General Application	Unsupported

	Settings	Settings	
Scan Site Directory Links	Configuration > General Application Settings	Central Administration > General Application Settings	Unsupported
The Site Directory	Configuration > General Application Settings	Central Administration > General Application Settings	Unsupported
Farm Search Administration	Configuration > General Application Settings	Central Administration > General Application Settings	Unsupported
Custom Properties	Configuration > Customization	N/A	Unsupported
Security			
Security Search Wizard Mode	Security > Contribute	N/A	Unsupported
Security Search Form Mode	Security > Contribute	N/A	Unsupported
Start with a Predefined Search	Security > Contribute	N/A	Unsupported
Configure Managed Accounts	Security > General Security	Central Administration > Security	Unsupported
Configure Service Accounts	Security > General Security	Central Administration > Security	Unsupported
Configure Password Changes Settings	Security > General Security	Central Administration > Security	Unsupported
Manage Trust	Security > General Security	Central Administration > Security	Unsupported
Manage Antivirus Settings	Security > General Security	Central Administration > Security	Unsupported
Define Blocked File Types	Security > General Security	Central Administration > Security	Unsupported
Manage Web Part Security	Security > General Security	Central Administration > Security	Unsupported
Clone User Permissions	Security > Permission	N/A	Unsupported
Import Configuration File	Security > Permission	N/A	Unsupported
Configure Information Rights Management	Security > Information Policy	Central Administration > Security	Unsupported
Configure Information Management Policy	Security > Information Policy	Central Administration > Security	Unsupported
Dead Account Cleaner	Security > Account	N/A	Unsupported

Web Application Level Operations

Operations	Location in DocAve	Location in SharePoint	Batch Settings
Management			
New Site Collection	Management > Contribute	Central Administration > Application Management	Supported
New Content Database	Management > Contribute	Central Administration > Application Management	Unsupported
Extend	Management > Contribute	Central Administration > Application Management	Unsupported
Delete Web Application	Management > Contribute	Central Administration > Application Management	Supported
Remove SharePoint from IIS Web Site	Management > Contribute	Central Administration > Application Management	Unsupported
Admin Search Wizard Mode	Management > Contribute	N/A	Supported
Admin Search Form Mode	Management > Contribute	N/A	Supported
Start with a Predefined Search	Management > Contribute	N/A	Supported
General Settings	Management > Manage	Central Administration > Application Management	Supported
Resource Throttling	Management > Manage	Central Administration > Application Management	Supported
Workflow	Management > Manage	Central Administration > Application Management	Supported
Outgoing Email	Management > Manage	Central Administration > Application Management	Supported
Mobile Account	Management > Manage	Central Administration > Application Management	Supported
Site Use and Deletions	Management > Manage	Central Administration > Application Management	Supported
Manage Features	Management > Manage	Central Administration > Application Management	Unsupported
Manage Paths	Management > Manage	Central Administration >	Unsupported

		Application Management	
Service Connections	Management > Manage	Central Administration > Application Management	Unsupported
Manage Content Databases	Management > Manage Content Databases	Central Administration > Application Management	Unsupported
Site Collection List	Management > Manage Content Databases	Central Administration > Application Management	Unsupported
Delete Orphan Sites	Management > Manage Content Databases	N/A	Supported
Search Web Parts	Management > Web Part	N/A	Supported
Job Monitor	Management > Statistics	N/A	N/A
Configuration			
Send to Connections	Configuration > External Service Connections	Central Administration > General Application Settings	Unsupported
Document Conversions	Configuration > External Service Connections	Central Administration > General Application Settings	Unsupported
SharePoint Designer Settings	Configuration > SharePoint Designer	Central Administration > General Application Settings	Unsupported
Alternate Access Mappings	Configuration > Web Application	Central Administration > Application Management	Unsupported
Custom Properties	Configuration > Customization	N/A	Supported
Security			
Authentication Providers	Security > General Settings	Central Administration > Application Management	Unsupported
Self-Service Site Creation	Security > General Settings	Central Administration > Application Management	Unsupported
Security Search Wizard Mode	Security > General Settings	N/A	Supported
Security Search Form	Security > General	N/A	Supported

Mode	Settings		
Start with a Predefined Search	Security > General Settings	N/A	Supported
Blocked File Types	Security > General Settings	Central Administration > Application Management	Unsupported
User Permissions	Security > General Settings	Central Administration > Application Management	Unsupported
Web Part Security	Security > General Settings	Central Administration > Application Management	Supported
Clone User Permissions	Security > Permission	N/A	Supported
User Policy	Security > Policy	Central Administration > Application Management	Unsupported
Anonymous Policy	Security > Policy	Central Administration > Application Management	Unsupported
Permission Policy	Security > Policy	Central Administration > Application Management	Unsupported
Dead Account Cleaner	Security > Account	N/A	Supported

Site Collection Level Operations

Operation	Location in DocAve	Location in SharePoint	Batch Settings
Management			
New	Management > Contribute	Login Site Collection > Site Actions > New Site	Supported
Move	Management > Contribute	N/A	Supported
Delete	Management > Contribute	Central Administration > Application Management	Supported
Admin Search Wizard Mode	Management > Contribute	N/A	Supported
Admin Search Form Mode	Management > Contribute	N/A	Supported

Start with a Predefined Search	Management > Contribute	N/A	Supported
Site Collection Features	Management > General Management	Login Site Collection > Site Actions > Site Settings	Supported
Portal Site Connection	Management > General Management	Login Site Collection > Site Actions > Site Settings	Supported
Content Type Publishing	Management > General Management	Login Site Collection > Site Actions > Site Settings	Unsupported
Web Part	Management > Galleries	Login Site Collection > Site Actions > Site Settings	Unsupported
Solutions	Management > Galleries	Login Site Collection > Site Actions > Site Settings	Unsupported
Themes	Management > Galleries	Login Site Collection > Site Actions > Site Settings	Unsupported
Site Columns	Management > Galleries	Login Site Collection > Site Actions > Site Settings	Unsupported
Check Broken Link	Management > Check	N/A	Supported
Search Web Parts	Management > Web Part	N/A	Supported
Job Monitor	Management > Statistics	N/A	N/A
Configuration			
Search Setting	Configuration > Search	Login Site Collection > Site Actions > Site Settings	Supported
Search Scopes	Configuration > Search	Login Site Collection > Site Actions > Site Settings	Unsupported
Search Keywords	Configuration > Search	Login Site Collection > Site Actions > Site Settings	Unsupported
Quotas and Locks	Configuration > General	Central Administration > Application Management	Supported
Visual Upgrade	Configuration > General	Login Site Collection > Site Actions > Site Settings	Unsupported
Deploy Site Maximum Depth	Configuration > General	N/A	Supported
RSS	Configuration > General	Login Site Collection > Site	Unsupported

		Actions > Site Settings	
Help Settings	Configuration > Help	Login Site Collection > Site Actions > Site Settings	Supported
SharePoint Designer Settings	Configuration > SharePoint Designer	Login Site Collection > Site Actions > Site Settings	Supported
Security			
People and Groups	Security > Contribute	Login Site Collection > Site Actions > Site Settings	Unsupported
Site Permissions	Security > Contribute	Login Site Collection > Site Actions > Site Settings	Unsupported
Security Search Wizard Mode	Security > Contribute	N/A	Supported
Security Search Form Mode	Security > Contribute	N/A	Supported
Start with a Predefined Search	Security > Contribute	N/A	Supported
Clone User Permissions	Security > Permission	N/A	Supported
Clone Site Permissions	Security > Permission	N/A	Unsupported
Grant Permissions	Security > Permission	Login Site Collection > Site Actions > Site Settings	Supported
Create Group	Security > Permission	Login Site Collection > Site Actions > Site Settings	Supported
Permission Levels	Security > Permission	Login Site Collection > Site Actions > Site Settings	Unsupported
Anonymous Access	Security > Permission	Login Site Collection > Site Actions > Site Settings	Supported
Export Group for Editing	Security > Permission	N/A	Supported
Site Collection Administrators	Security > Administrators	Login Site Collection > Site Actions > Site Settings	Supported
Dead Account Cleaner	Security > Account	N/A	Supported

Permission Tools			
Grant Permissions	Permission Tools > Grant *Note: After selecting Site Permissions feature, the Permission Tools tab will be enabled.	Login Site Collection > Site Actions > Site Settings	Supported
Create Group	Permission Tools > Grant	Login Site Collection > Site Actions > Site Settings	Supported
Edit User Permissions	Permission Tools > Modify	Login Site Collection > Site Actions > Site Settings	Supported
Remove User Permissions	Permission Tools > Modify	Login Site Collection > Site Actions > Site Settings	Supported
Delete User/Groups from Site Collection	Permission Tools > Modify	Login Site Collection > Site Actions > Site Settings	Supported
Anonymous Access	Permission Tools > Manage	Login Site Collection > Site Actions > Site Settings	N/A
Permission Levels	Permission Tools > Manage	Login Site Collection > Site Actions > Site Settings	N/A
Site Collection Administrators	Permission Tools > Manage	Login Site Collection > Site Actions > Site Settings	N/A

Sub-site Level Operations

Operation	Location in DocAve	Location in SharePoint	Batch Settings
Management			
New Subsite	Management > Contribute	Login a Site > Site Actions > New Site	Supported
New List\Library	Management > Contribute	Login a Site > Site Actions > More Options	Supported
Delete	Management > Contribute	Login a Site > Site Actions > Site Settings	Supported
Admin Search Wizard Mode	Management > Contribute	N/A	Supported
Admin Search Form Mode	Management > Contribute	N/A	Supported
Start with a Predefined Search	Management > Contribute	N/A	Supported

Site Features	Management > General Management	Login a Site > Site Actions > Site Settings	Supported
Reset To Site Definition	Management > General Management	Login a Site > Site Actions > Site Settings	Unsupported
Regional Settings	Management > General Management	Login a Site > Site Actions > Site Settings	Supported
Site Columns	Management > Galleries	Login a Site > Site Actions > Site Settings	Unsupported
Site Content Types	Management > Galleries	Login a Site > Site Actions > Site Settings	Unsupported
Master Page	Management > Galleries	Login a Site > Site Actions > Site Settings	Unsupported
Check Broken Link	Management > Check	N/A	Supported
Search Web Parts	Management > Web Part	N/A	Supported
Job Monitor	Management > Statistics	N/A	N/A
Configuration			
RSS Setting	Configuration > General	Login a Site > Site Actions > Site Settings	Unsupported
Search And Offline Availability	Configuration > General	Login a Site > Site Actions > Site Settings	Supported
Related Links Scope Settings	Configuration > General	Login a Site > Site Actions > Site Settings	Unsupported
Title, Description, and Icon	Configuration > Look and Feel	Login a Site > Site Actions > Site Settings	Unsupported
Quick Launch	Configuration > Look and Feel	Login a Site > Site Actions > Site Settings	Unsupported
Top Link Bar	Configuration > Look and Feel	Login a Site > Site Actions > Site Settings	Unsupported
Tree View	Configuration > Look and Feel	Login a Site > Site Actions > Site Settings	Unsupported
Site Theme	Configuration > Look and Feel	Login a Site > Site Actions > Site Settings	Supported
Custom Properties	Configuration > Customization	N/A	Supported
Security			
People and Groups	Security > Contribute	Login a Site > Site Actions > Site Settings	Unsupported
Site Permissions	Security > Contribute	Login a Site > Site Actions > Site Settings	Unsupported
Security Search Wizard Mode	Security > Contribute	N/A	Supported

Security Search Form Mode	Security > Contribute	N/A	Supported
Start with a Predefined Search	Security > Contribute	N/A	Supported
Clone User Permissions	Security > Permission	N/A	Supported
Clone Site Permissions	Security > Permission	N/A	Unsupported
Grant Permissions	Security > Permission	Login a Site > Site Actions > Site Settings	Supported
Create Group	Security > Permission	Login a Site > Site Actions > Site Settings	Supported
Permission Levels	Security > Permission	Login a Site > Site Actions > Site Settings	Unsupported
Anonymous Access	Security > Permission	Login a Site > Site Actions > Site Settings	Supported
Stop Inheriting Permissions	Security > Permission	Login a Site > Site Actions > Site Settings	Supported
Inherit Permissions	Security > Permission	Login a Site > Site Actions > Site Settings	Supported
User Alerts	Security > Share and Track	Login a Site > Site Actions > Site Settings	Unsupported
Search Alert	Security > Share and Track	N/A	Unsupported
Dead Account Cleaner	Security > Account	N/A	Supported
Permission Tools			
Grant Permissions	Permission Tools > Grant *Note: after selecting Site Permissions feature, the Permission Tools tab will be enabled.	Login Site Collection > Site Actions > Site Settings	Supported
Create Group	Permission Tools > Grant	Login Site Collection > Site Actions > Site Settings	Supported
Inherit Permissions	Permission Tools > Inheritance	Login Site Collection > Site Actions > Site Settings	N/A
Stop Inheriting Permissions	Permission Tools > Inheritance	Login Site Collection > Site Actions > Site Settings	N/A
Edit User Permissions	Permission Tools > Modify	Login Site Collection > Site Actions > Site Settings	Supported
Remove User Permissions	Permission Tools > Modify	Login Site Collection > Site Actions > Site Settings	Supported

Permission Levels	Permission Tools > Manage	Login Site Collection > Site Actions > Site Settings	N/A
-------------------	---------------------------	--	-----

List/Library Level Operations

Operation	Location in DocAve	Location in SharePoint	Batch Settings
Management			
New Folder	Management > Contribute	Access a library > Documents > New Folder	Unsupported
Delete	Management > Contribute	Access a list/library > List/Library > List/Library Settings	Supported
Admin Search Wizard Mode	Management > Contribute	N/A	Supported
Admin Search Form Mode	Management > Contribute	N/A	Supported
Start with a Predefined Search	Management > Contribute	N/A	Supported
No checked In Version Files	Management > General Management	Access a library > Library > Library Settings	Unsupported
Workflow Settings	Management > General Management	Access a list/library > List/Library	Unsupported
Metadata and Keywords Settings	Management > General Management	Access a list/library > List/Library > List/Library Settings	Unsupported
Indexed Columns	Management > Columns	Access a list/library > List/Library > List/Library Settings	
Job Monitor	Management > Statistics	N/A	N/A
Configuration			
Versioning Settings	Configuration > General	Access a list/library > List/Library > List/Library Settings	Supported
Advanced Settings	Configuration > General	Access a list/library > List/Library > List/Library Settings Access a list/library > List/Library >	Supported

		List/Library Settings	
Validation Settings	Configuration > General	Access a list/library > List/Library > List/Library Settings	Unsupported
Column Default Value Settings	Configuration > General	Access a library > Library > Library Settings	
Rating Settings	Configuration > General	Access a list/library > List/Library > List/Library Settings	Supported
Audience Targeting Settings	Configuration > General	Access a list/library > List/Library > List/Library Settings	Unsupported
Metadata Navigation Settings	Configuration > General	Access a list/library > List/Library > List/Library Settings	Unsupported
Pre-location View Settings	Configuration > General	Access a list/library > List/Library > List/Library Settings	Unsupported
RSS Setting	Configuration > General	Access a list/library > List/Library > List/Library Settings	Unsupported
Title, Description and Navigation	Configuration > Look and Feel	Access a list/library > List/Library > List/Library Settings	Unsupported
Security			
List Permissions	Security > Contribute	Access a list/library > List/Library > List/Library Permissions	Unsupported
Security Search Wizard Mode	Security > Contribute	N/A	Supported
Security Search Form Mode	Security > Contribute	N/A	Supported
Start with a Predefined Search	Security > Contribute	N/A	Supported
Clone User Permissions	Security > Permission	N/A	Supported
Clone List/Library Permissions	Security > Permission	N/A	Unsupported
Grant Permissions	Security > Permission	Access a list/library > List/Library > List/Library Permissions	Supported
Stop Inheriting	Security > Permission	Access a list/library >	Supported

Permissions		List/Library > List/Library Permissions	
Inherit Permissions	Security > Permission	Access a list/library > List/Library > List/Library Permissions	Supported
Start alert on this library/list	Security > Share and Track	Access a list/library > List/Library > Alert Me	Supported
Manage My Alert	Security > Share and Track	Access a list/library > List/Library > Alert Me	Unsupported
Permission Tools			
Inherit Permissions	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	N/A
Stop Inheriting Permissions	Permission Tools > Inheritance	Access a list/library > List/Library > List/Library Permissions	N/A
Grant Permissions	Permission Tools > Grant	Access a list/library > List/Library > List/Library Permissions	Supported
Edit User Permissions	Permission Tools > Modify	Access a list/library > List/Library > List/Library Permissions	Supported
Remove User Permissions	Permission Tools > Modify	Access a list/library > List/Library > List/Library Permissions	Supported

Folder Level Operations

Operation	Location in DocAve	Location in SharePoint	Batch Settings
Management			
New Folder	Management > Contribute	Access a folder > Documents > New Folder	Supported
Delete	Management > Contribute	Select a folder > Documents > Delete	Supported
Admin Search Wizard Mode	Management > Contribute	N/A	Supported
Admin Search Form Mode	Management > Contribute	N/A	Supported
Start with a	Management >	N/A	Supported

Predefined Search	Contribute		
View Properties	Management > Contribute	Select a folder > Documents > View Properties	Supported
Job Monitor	Management > Statistics	N/A	N/A
View Properties			
Edit	View Properties > Management *Note: After selecting View Properties feature, the tab is enabled.	Select a folder > Documents > Edit Properties	Unsupported
Security			
Folder Permissions	Security > Contribute	Select a folder > Documents > Document Permissions	Unsupported
Security Search Wizard Mode	Security > Contribute	N/A	Supported
Security Search Form Mode	Security > Contribute	N/A	Supported
Start with a Predefined Search	Security > Contribute	N/A	Supported
Clone User Permissions	Security > Permission	N/A	Supported
Clone Folder Permissions	Security > Permission	N/A	Unsupported
Grant Permissions	Security > Permission	Select a folder > Documents > Document Permissions	Supported
Stop Inheriting Permissions	Security > Permission	Select a folder > Documents > Document Permissions	Supported
Inherit Permissions	Security > Permission	Select a folder > Documents > Document Permissions	Supported
Alert Me	Security > Alert	Select a folder > Documents > Alert Me	Supported
Permission Tools			
Inherit Permissions	Permission Tools > Inheritance *Note: after selecting Folder Permissions feature, the Permission	Select a folder > Documents > Document Permissions	N/A

	Tools tab will be enabled.		
Stop Inheriting Permissions	Permission Tools > Inheritance	Select a folder > Documents > Document Permissions	N/A
Grant Permissions	Permission Tools > Grant	Select a folder > Documents > Document Permissions	Supported
Edit User Permissions	Permission Tools > Modify	Select a folder > Documents > Document Permissions	Supported
Remove User Permissions	Permission Tools > Modify	Select a folder > Documents > Document Permissions	Supported

Item Level Operations

Operation	Location in DocAve	Location in SharePoint	Batch Settings
Management			
Delete	Management > Contribute	Select an item > Items > Delete Item	Supported
Admin Search Wizard Mode	Management > Contribute	N/A	Supported
Admin Search Form Mode	Management > Contribute	N/A	Supported
Start with a Predefined Search	Management > Contribute	N/A	Supported
Job Monitor	Management > Statistics	N/A	N/A
Security			
Item Permissions	Security > Contribute	Select an item > Items > Item Permissions	Unsupported
Security Search Wizard Mode	Security > Contribute	N/A	Supported
Security Search Form Mode	Security > Contribute	N/A	Supported
Start with a Predefined Search	Security > Contribute	N/A	Supported
Stop Inheriting Permissions	Security > Permission	Select an item > Items > Item Permissions	Supported
Inherit Permissions	Security > Permission	Select an item > Items > Item Permissions	Supported
Grant Permissions	Security > Permission	Select an item > Items >	Supported

		Item Permissions	
Alert Me	Security > Alert	Select an item > Items > Alert Me	Supported
Permission Tools			
Inherit Permissions	Permission Tools > Inheritance *Note: Selecting Item Permissions enables Permission Tools tab.	Select an item > Items > Item Permissions	N/A
Stop Inheriting Permissions	Permission Tools > Inheritance	Select an item > Items > Item Permissions	N/A
Grant Permissions	Permission Tools > Grant	Select an item > Items > Item Permissions	Supported
Edit User Permissions	Permission Tools > Modify	Select an item > Items > Item Permissions	Supported
Remove User Permissions	Permission Tools > Modify	Select an item > Items > Item Permissions	Supported

Appendix C

Security Search Result

Operation	Location in DocAve	Location in SharePoint	Batch Settings
Tools(Group)			
Created Group	Tools > Contribute	N/A	Supported
Add Users	Tools > Contribute	N/A	Supported
Group Settings	Tools > Contribute	N/A	Supported
Edit Group Permissions	Tools > Contribute	N/A	Supported
Remove Group Permissions	Tools > Contribute	N/A	Supported
Download Report	Tools > Export and Import	N/A	N/A
Export for Editing	Tools > Export and Import	N/A	N/A
Import Configuration File	Tools > Export and Import	N/A	N/A
Tools(User)			
Add Users	Tools > Contribute	N/A	Supported
Edit User Permissions	Tools > Contribute	N/A	
Remove User	Tools > Contribute	N/A	Supported

Permissions			
Delete Users	Tools > Contribute	N/A	Supported
Download Report	Tools > Export and Import	N/A	N/A
Export for Editing	Tools > Export and Import	N/A	N/A
Import Configuration File	Tools > Export and Import	N/A	N/A

Index

- Admin Search**, 12
- Admin Search Form Mode**, 13
- Admin Search Wizard Mode, 12
- Administration**, 8
- Alert Me**, 20
- Central Admin**, 8
- Change Content Database**, 17
- Check Broken Link**, 18
- Clone Permissions**, 26
- Clone Site Permissions, 27
- Clone User Permissions, 26
- Configuration**, 16
- Dead Account Cleaner, 28
- Delete**, 21
- Delete Orphan Sites**, 21
- Delete Web Application, 21
- Deploy Site Maximum Depth**, 16
- Download Report**, 32
- Export for Editing**, 31
- Extend**, 17
- Import Configuration File**, 31, 32
- Management tab**, 9
- Maximum Depth**, 16
- Move**, 17
- New Content Database, 16
- New Site Collection**, 16
- People and Groups**, 11
- Plan Mode, 28
- Right-Click Operations for Each Level, 24
- Scan Mode, 29
- Scan now on the front-end**, 21
- Scan on the back-end and save as a plan**, 21
- Scope panel**, 10
- Search Alert**, 20
- Search Web Parts**, 19
- Security Search Form Mode**, 15
- Security Search Wizard Mode, 13
- Site Collection List**, 11
- Site Permissions, 11
- Start with a Predefined Search**, 15
- Tools**, 32
- Web Part Management**, 20

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 AvePoint, Inc. All rights reserved. All materials contained in this publication are protected by United States copyright law 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.

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 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.
3 Second Street
Jersey City, NJ 07311
USA