DocAve® 6 Control Panel

Reference Guide

Service Pack 5

Revision B

Issued February 2015

Table of Contents

What's New in this Guide 7

About Control Panel 8

Submitting Documentation Feedback to AvePoint 9

Before You Begin 10

- AvePoint's Testing Policy and Environment Support 10
  - Supported Hardware 10
  - Supported Backup and Recovery 10
  - Notable Environment Exceptions 11
- Configuration 11
- Agents 11

Getting Started 12

- Launching Control Panel 12
- Navigating DocAve 13
- Understanding Control Panel 15
- Accessing Control Panel 15

System Settings 16

- Monitor 16
  - Using Manager Monitor 16
  - Using Agent Monitor 19
- System Options 23
  - Configuring General Settings 23
  - Configuring Security Settings 24
  - Viewing Security Information 26
- Authentication and Account Manager 26
  - Authentication Manager 27
  - Account Manager 33
- License Manager 56
  - Viewing License Information 56
  - Importing and Exporting License Files 58

Configuring License Renewal Notifications 58
Configuring SharePoint Server Usage 59
Update Manager 60
Configuring Update Settings 60
Managing Updates 61
Reviewing Installation History of Updates 62
Application Settings 64
Agent Groups 64
Managing Agent Groups 64
User Notification Settings 67
Configuring Outgoing E-mail Settings 67
Configuring Notification E-mail Settings 67
Job Manager 69
Job Pruning 69
Job Performance Alert 73
Log Manager 74
Configuring Log Settings 74
Scrubbing the Logs 75
Collecting Logs 77
Registered SharePoint Sites 78
Manual Input Mode 79
Scan Mode 84
Office 365 Account Profile Manager 87
Agent Proxy Settings 88
Profile Manager 90
Security Profile 90
Managed Account Profile 91
Settings for Specific Products/Modules 94
Solution Manager 94
Managing Solutions 94
Maintaining Solutions 96
Solution Description 96

Storage Configuration 100
Physical Device 100
Logical Device 127
Storage Policy 130
Data Manager 135
Importing Data from DocAve 5 to DocAve 6 135
Importing Data from DocAve 6 to DocAve 6 Service Pack 1 or Later Versions 146
Converting 3rd Party Tool Stub to DocAve Stub 152
Index Manager 154
Creating an Index Profile 154
Configuring Workday for the Index Profile 155
Export Location 156
Managing Export Locations 156
Configuring Export Locations 157
Filter Policy 157
Managing Filter Policies 157
Configuring Filter Policies 158
Host Profile 159
Creating a Host Profile 159
Viewing Details about a Host Profile 161
Editing a Host Profile 161
Deleting Host Profiles 161
Mapping Manager 162
Domain Mapping 163
User Mapping 165
Language Mapping 167
Column Mapping 168
Content Type Mapping 172
Template Mapping 173
Group Mapping 174
List Name Mapping 175
Plan Group 178

Security Trimming for Plan Group 178
Managing Plan Group 178
Creating a Plan Group 179
Configuring the Add Schedule Interface 182
Configuring the Default Settings Section 183
Appendix A: Examples of Filter Policies 186
Site Collection Level 186
Site Level 194
List/Library Level 202
Folder Level 206
Item Level 211
Document Level 221
Attachment Level 227
Appendix B: Template Name and Template ID 230
Appendix C: Hot Key Functionality 232
Using Hot Keys Mode in Control Panel 232
Manager Monitor 232
Agent Monitor 232
System Option 233
Authentication Manager 233
Account Manager 234
License Manager 236
Update Manager 237
Agent Groups 237
User Notification Setting 237
Job Pruning 238
Job Performance Alert 238
Log Manager 239
Registered SharePoint Sites 239
Office 365 Account Profile Manager 240
Agent Proxy Settings 240
Security Profile 241

Managed Account Profile 241
Solution Manager 241
Storage Configuration 242
Index Manager 242
Export Location 243
Filter Policy 243
Host Profile 243
Mapping Manager 244
Using Hot Keys Mode in Plan Group 247
Notices and Copyright Information 249

What's New in this Guide

- New feature – Host Profile Manager. Use Host Profile to store the necessary information so that you can connect to the host successfully. Host Profile can be used in Platform Backup & Restore module and VM Backup & Restore module.
- New feature – Importing AD Users in Bulk in Account Manager. We can use this function to import AD users in bulk, which is a more efficient way to add AD users to system groups and tenant groups.
- Improvements to Update Manager.
- DocAve now supports Box, NFS and IBM Storwize as Physical Devices for storage.

About Control Panel

The DocAve Control Panel is the central interface for managing DocAve and how it interacts with your SharePoint environments.

Control Panel is also integrated into other DocAve products, which enables you to configure relevant settings without having to leave the interface of the module you are using.

Submitting Documentation Feedback to AvePoint

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

Before You Begin

Refer to the sections below for the system requirements for Control Panel.

AvePoint's Testing Policy and Environment Support

Supported Hardware

AvePoint is committed to maintaining a hardware agnostic platform to ensure that DocAve operates on common Windows file sharing and virtualization platforms. To ensure that DocAve is hardware agnostic, AvePoint tests hardware that is intended to support SharePoint and DocAve infrastructure, storage targets, and hardware-based backup and recovery solutions, as supported by AvePoint's partnerships. AvePoint directly integrates with the following platforms: any Net Share, IBM Storwize Family, FTP, Amazon S3, AT&T Synaptic, Caringo Storage, Del DX Storage, EMC Centra, HDS Hitachi Content Platform, Rackspace Cloud Files, TSM, and Windows Azure Storage.

All other hardware platforms that support UNC addressable storage devices are supported.

***Note:** Most of the hardware partnerships referenced in this guide are intended to make use of advanced functionality (such as snapshot mirroring, BLOB snapshots, indexing, long-term storage, WORM storage, etc.), and are not indications that any changes to the product are required for basic support. In most cases, hardware can be supported with no change to the product.

Supported Backup and Recovery

DocAve supports BLOB backup storage according to the list of hardware platforms above. BLOB snapshot functionally, however, is currently only supported on OEM versions and NetApp hardware.

DocAve supports SQL content and Application database backups via the SharePoint Volume Shadow Copy Service (VSS) on all Windows and SQL server platforms listed above. DocAve also supports snapshot-based SharePoint VSS on all hardware listed above where the hardware partner has certified support with Microsoft.

DocAve supports application and configuration server backups for all the supported software environments listed above. DocAve 6 supports VM backup via Hyper-V/VMWare for the following operating systems: Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Microsoft Hyper–V Server 2012 R2.

Notable Environment Exceptions

The following are notable exceptions to the supported DocAve environments. The following represent environment level support information, not feature level support. Feature level support, specific to each feature, is described throughout this guide where applicable.

- DocAve 6 does not support creating websites in an existing application pool using IIS7 Classic Managed Pipeline Mode when .NET 4.0 is also in use.
- The DocAve 6 Report Service only supports Microsoft SQL Server as the Database Type for Report Service databases.

Configuration

To use Control Panel, the DocAve 6 platform must be installed and configured properly on your farm. Control Panel 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 Control Panel commands to function properly.

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

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

Getting Started

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

Launching Control Panel

To launch Control Panel and access its functionality, follow the instructions below:

1. Log into DocAve. If you are already in the software, click the **DocAve** tab.
2. From the **DocAve** tab, click **Control Panel** to launch Control Panel.

   Alternatively, you can click the Control Panel ( ) button from anywhere within the DocAve software to launch Control Panel.

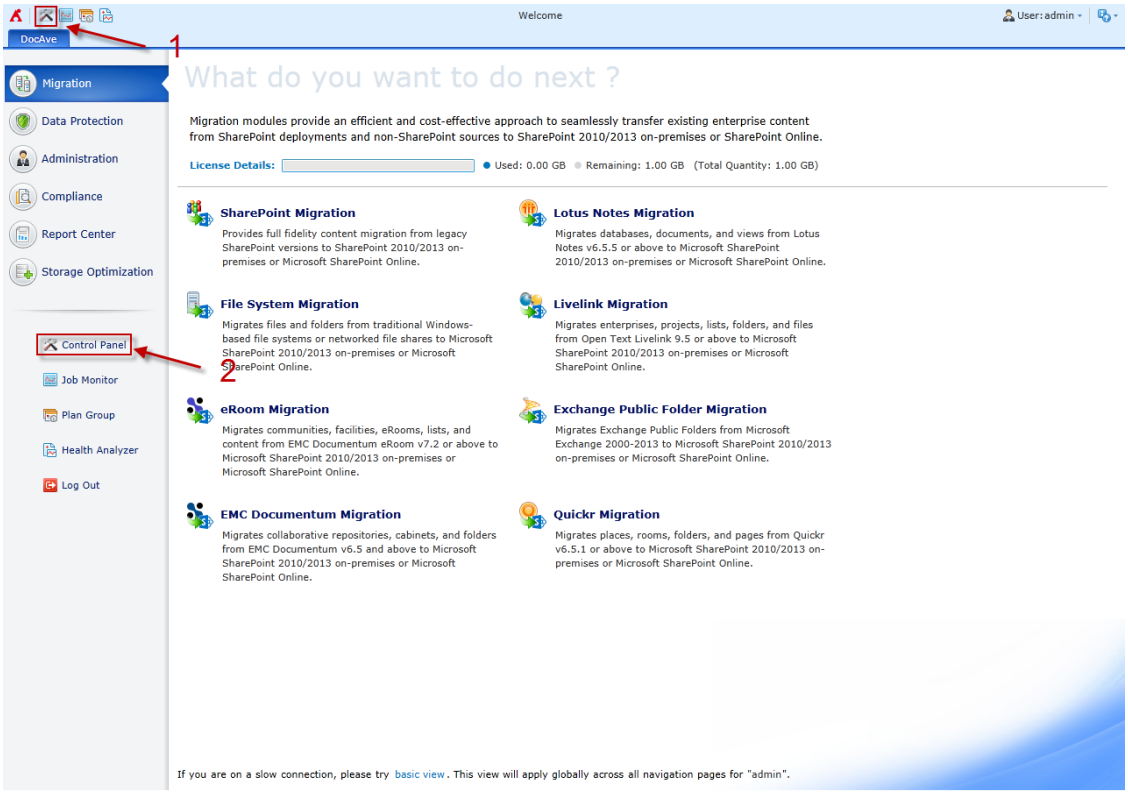

Figure 1: Control Panel icon on DocAve homepage.

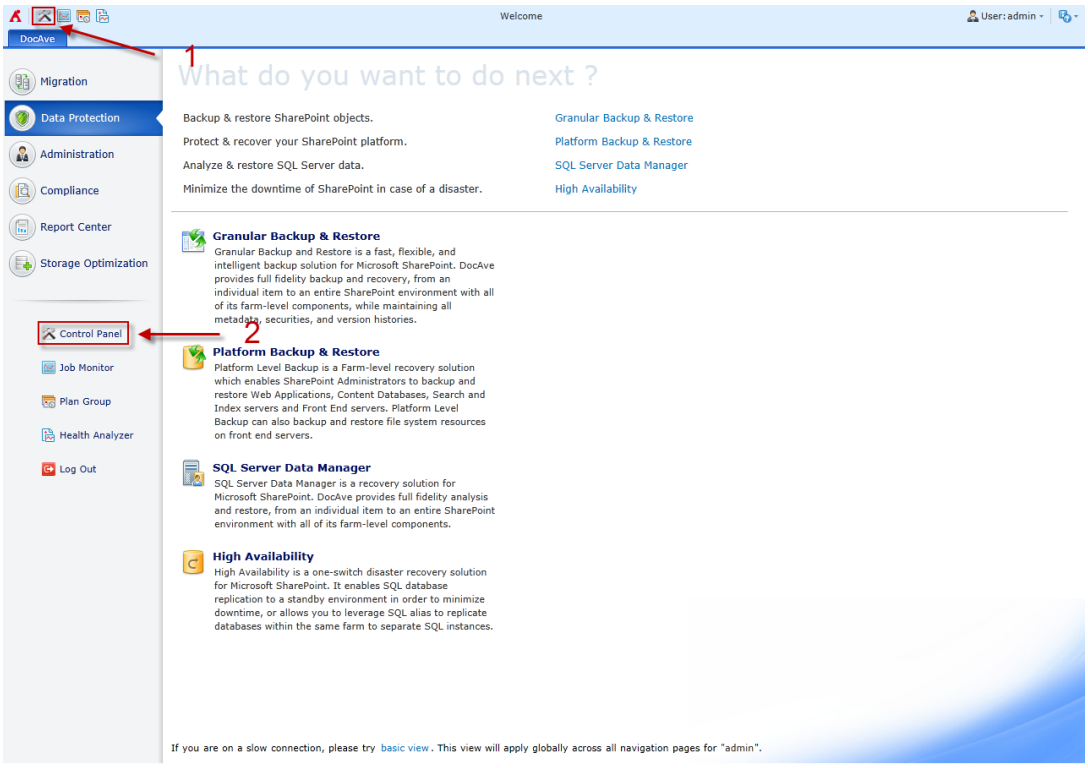

Figure 2: DocAve module launch window.

Navigating DocAve

DocAve mimics the look and feel of many Windows products, making for an intuitive and familiar working environment. While there are many windows, pop-up displays, and messages within DocAve products, they share similar features and are navigated in the same ways.

Below is a sample window in DocAve. It features a familiar, dynamic ribbon, and a searchable, content list view.

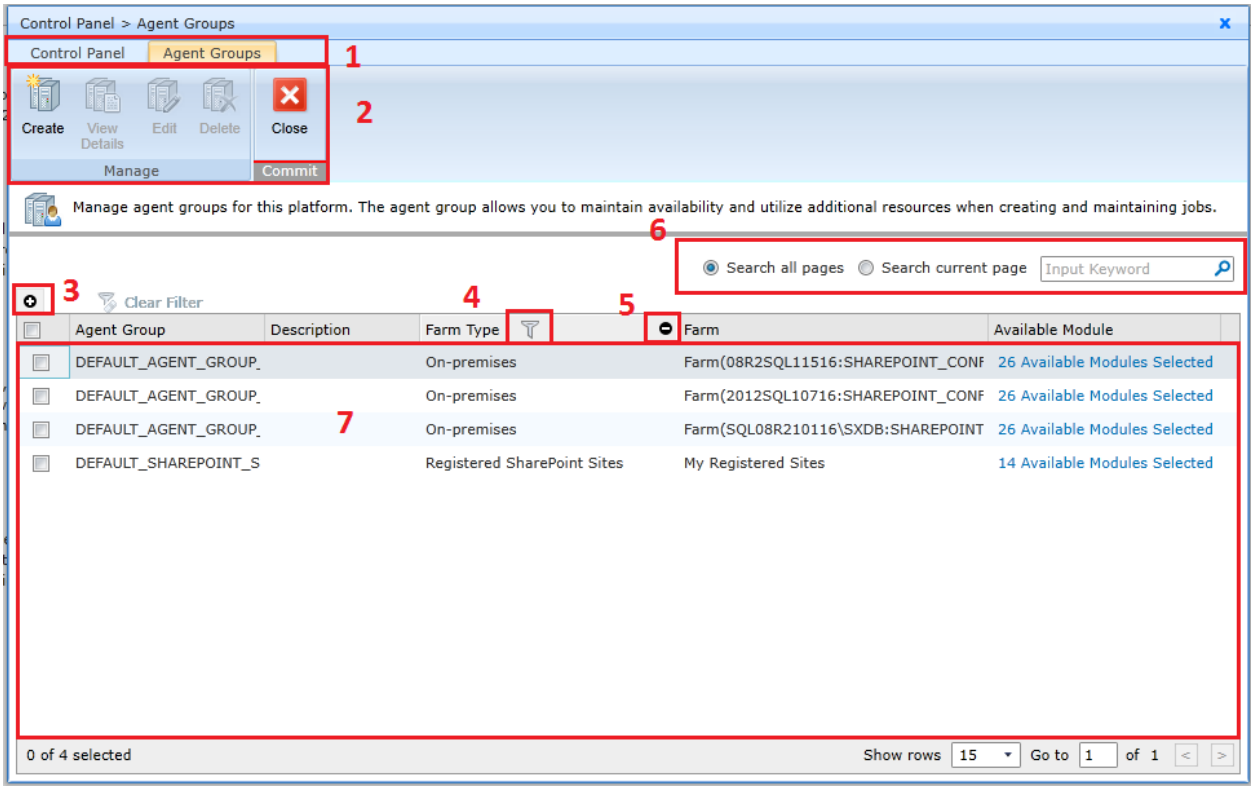

Figure 3: Navigating DocAve.

1. Ribbon Tabs—Allows users to navigate between the Control Panel page and other active Control Panel components.
2. Ribbon Panes – Allows users to access the functionality of the active DocAve module.
3. Manage columns (⊕) – Allows users to manage which columns are displayed in the list. Click the manage columns (⊕) button, and then select the checkbox next to the column name in the drop-down list. Filter the column ( ) – Allows users to filter the information in the List View. Click the filter the column ( ) button next to the column and then select the checkbox next to the column name.
4. Hide the column (⊖) – Allows users to hide the selected column.
5. **Search** – Allows users to search the List View pane for a keyword or phrase. You can select **Search all pages** or **Search current page** to define the search scope.
   ***Note**: The search function is not case sensitive.

6. Management Pane – Displays the actionable content of the DocAve module.

Understanding Control Panel

Control Panel has three key groups of components:

- **System Settings** – View and manage your DocAve settings, Managers, Agents, authentication, licenses, and product version. All of these functions are performed in the Control Panel so that you can easily access them without leaving the interface for your current task in DocAve.
- **Application Settings** – Configure settings affecting common tasks performed by all DocAve products. All of these settings are configured in the Control Panel so that you can easily access them without leaving the interface for your current task in DocAve.
- **Specific Products Settings** – Certain products in DocAve utilize preset configurations for certain functionalities. While these settings may not affect all DocAve products, all of these settings are configured in the Control Panel because they can be leveraged by more than one product.

Accessing Control Panel

Since features in Control Panel overlap with so many products, it is important that it is easily accessible but not disruptive of your current task. While there are many ways to access Control Panel, the interface opens as a pop-up window so that you can remain on whichever page you are on. When you are finished configuring settings in Control Panel, closing it will return you to the page you were on.

To access Control Panel, complete the following steps:

1. Click the **DocAve** tab, and then click **Control Panel** in the left panel to launch Control Panel.
2. At any point while in DocAve, click the **Control Panel** ( ) button in the upper-left corner to launch Control Panel.
3. While in the interface of a certain product, if the product utilizes a feature in Control Panel, click on that feature on the ribbon of the product page to bring up the Control Panel pop-up window with the appropriate tab open.
4. Whenever you are finished configuring settings in Control Panel, close the window to return to the previous screen you were on.

System Settings

General System Settings in Control Panel allow you to customize the way DocAve interacts with your SharePoint environment. Here you can manage DocAve Managers and Agents, configure DocAve settings, and perform DocAve administrative tasks.

- **Monitor** – DocAve Control Panel includes a Manager and an Agent Monitors. These settings provide you with control over the DocAve Managers and Agents installed on your SharePoint environment.
- **System Options** – In System Options, you can configure General and Security Settings.
- **Managers** – In Control Panel, there are Authentication and DocAve managers; Authentication managers include the Authentication and the Account Managers, which gives you control over who has access to and what they can do in DocAve. DocAve managers include the License and the Update Managers. These let you view and manage which DocAve products you have access to, and what version of DocAve you are using.

Monitor

The monitor features in DocAve Control Panel allow you to view and manage the DocAve Manager and DocAve Agent services:

- **Manager Monitor** – View and configure your DocAve Manager services currently installed on your SharePoint environment. With **Manager Monitor**, you can also perform basic maintenance operations on your Manager services if a Manager service ever becomes unresponsive or is having issues. You can also temporarily disable the DocAve Manager services to perform server maintenance.
- **Agent Monitor** – View and configure your DocAve Agents currently installed on your SharePoint environment. This can be useful if there is a change in personnel, and the SharePoint account that the Agent uses to communicate with SharePoint needs to be changed. With Agent Monitor, you can also perform basic maintenance operations on your Agents if an Agent ever becomes unresponsive or is having issues, or temporarily disable the DocAve Agent service to perform server maintenance.

Using Manager Monitor

To access **Manager Monitor**, in the **Control Panel** interface, click **Manager Monitor** under the **Monitor** heading. In **Manager Monitor**, you will see a list of Manager services which have been registered to the current DocAve Control service. Manager services include the Control service, Media service, and Report service.

Refer to the following sections on how to manage the Manager services.

Configuring Media Service

Only the Media services can be configured in **Manager Monitor**. Once your Manager services are appropriately displayed, select a Media service by selecting the checkbox next to the **Service Name**, and then click **Configure** on the ribbon. In the **Configure** interface, configure the following settings:

1. **Cache Location** – Saves the index database which stores the index of the backup data. By default, the cache location is set to: *…\AvePoint\DocAve6\Manager\Media\Cache*.

    - **Add Cache Location** – Creates a new cache location. Click the **Add Cache Location** link in the **Cache Location** field or **Add Cache Location** on the ribbon to create a new cache location. The **Add Cache Location** interface appears. Configure the following settings:

        i. **Device Type** – Choose to store the caches in a local path or a UNC path.

        ***Note:** If your environment is the Media service High Availability environment, you can only select the **UNC Path** as the **Device Type**; otherwise, the test will fail.

        ii. **Destination** – Select the directory where you are about to store the caches.

            - If you select **Local Path** in the **Device Type** field, enter a path in the **Local path** text box.
            - If you select **UNC Path** in the **Device Type** field, enter a path in the **UNC path** text box and select a managed account profile from the drop-down list to access the entered UNC path.

        iii. Click **Validation Test** to test the entered path is valid.

        iv. Click **Save** to save the cache location or click **Cancel** to exit the current page without saving any configuration.

        If more than one cache location is configured for the Media service, DocAve will store cache data according to the order of the cache locations listed here. Change the order in which the cache locations are listed in by selecting its desired place in the list from the corresponding drop-down menu under the **Order** column. Once all of the cache locations are full, the oldest data will be deleted to make room for new data.

    - **Edit Cache Location** – Edits an existing cache location. Select a cache location by selecting the corresponding checkbox. Click **Edit Cache Location** on the ribbon to edit it. The editing steps are the same as the creating steps; refer to the creating steps above for more information.
    - **Refresh** – Refreshes one or more cache locations to view the usage information. Select one or more cache locations by selecting the corresponding checkboxes. Click the **Refresh** link or **Refresh** on the ribbon to refresh the selected cache locations. The usage information is displayed in the **Free Space** column.

- **Delete** – Deletes one or more cache locations. Select one or more cache locations by selecting the corresponding checkboxes. Click the delete ( ) button or **Delete** on the ribbon to delete the selected cache locations.

  ***Note:** The Media service must have at least one cache location. If you attempt to delete the only cache location configured for a Media service, an error message will pop up, and the selected cache location will not be deleted.

2. **Threshold** – Enter the cache location free space threshold. The threshold you set will be the lowest amount of free space a cache location can have before either another cache location (if configured) is used, or the data is deleted. To set the **Threshold**, enter the number in Megabytes into the corresponding text box.

   ***Note:** By default, the threshold is 1024 MB. If the cache location is in the system disk, keep at least 1024 MB of free space to ensure that the performance of the operating system is not affected.

3. Click **Save** on the ribbon to save the configurations and return to the **Manager Monitor** interface, or click **Cancel** to return to the **Manager Monitor** interface without saving any configurations.

Viewing Details of the Manager Services

Select a Control, Media, or Report service by selecting the corresponding checkbox, and then click **View Details** on the ribbon to view the detailed information of the selected Manager service.

Configuring Notification Settings for the Manager Services

If you have configured the e-mail notification settings for the Manager service, the specified recipients in the selected notification profile will be sent an e-mail when the Manager service is inactive. To do so, complete the following steps:

1. Select one or more Manager services by selecting the corresponding checkboxes, and then click **Notification Selection** on the ribbon. The **Notification Selection** interface appears.
2. Select a previously configured notification profile from the drop-down menu or select **New Notification Profile** to set up a new e-mail notification profile. For more information about how to configure notification, refer to User Notification Settings.
3. Click **Save** to save the configuration and return to the **Manager Monitor** interface or click **Cancel** to return to the **Manager Monitor** interface without saving any configurations.

Restarting the Manager Services

Select one or more Media or Report services, and then click **Restart** on the ribbon to restart the selected Manager services. This is useful in situations where the Manager is sluggish, or if a job it is running hangs. You can restart the Manager service and try again.

***Note**: Any jobs that are running when you restart the Manager services may fail.

Removing the Manager Services

Select one or more down Media or Report services, and then click **Remove** on the ribbon to remove the selected Manager services. The removed Manager service will no longer be used by the current Control service. You can only remove Manager services that have a down arrow ( ) button in the **Status** column.

***Note:** Removing the service does not uninstall the Manager service.

Deactivating the Manager Services

Select one or more Media or Report services, and then click **Deactivate** on the ribbon to deactivate the selected Manager service. Once the Manager service is deactivated, it is marked as **Inactive** and will not be used by the current Control service. However, the deactivated service will still run normally. This is useful when you want to perform maintenance on a specified DocAve Manager server.

***Note**: Any jobs that are running when you deactivate the Manager service may fail.

Activating the Manager Services

Select one or more deactivated Media or Report services, and then click **Activate** on the ribbon to activate the selected Manager services. Once the Manager service is activated, it is marked as **Active** and will be used by the current Control service.

When you are finished viewing and managing your Manager services, click **Close** on the ribbon to close the **Manager Monitor** interface and return to the **Control Panel** interface.

Using Agent Monitor

To access **Agent Monitor**, in the **Control Panel** interface, click **Agent Monitor** under the **Monitor** heading. In **Agent Monitor**, you will see a list of DocAve Agents which have been registered to the current DocAve Control service.

Once your DocAve Agents are appropriately displayed, you can select an Agent by selecting the checkbox next to the **Agent Name**, and then click:

- **Configure** – Once you select an Agent, this button will become available. Click **Configure** on the ribbon to access the **Agent Configuration** interface. Here you can configure the SharePoint account, Agent type, job restriction, and temporary buffer for the Agent.
    - **SharePoint Account** – The SharePoint account is used by the DocAve Agent to provide DocAve with access and control to your SharePoint environment. Select a managed account profile from the drop-down list, or click **New Managed Account Profile** to create a new one. For more information on how to create a new managed account profile, refer to Managing the Managed Account Profile.
    - **Agent Type Configuration** – In order to use a certain product, the corresponding Agent type must first be configured. Before selecting the product, the necessary

Agents for that product must already be installed. For more information, refer to the DocAve 6 Installation Guide.

To configure the Agent type for the Agent, select the checkbox next to the corresponding product. You can navigate through the different product suites that are enabled for you by clicking on the name of the suite. Click **On-premises** to configure the Agent type on your SharePoint on-premises environment.

***Note:** Since **Cloud Connect** module shares the same Agent type as the **Connector** module, select the **Connector** checkbox if you want to select the **Cloud Connect** module.

Switch to the **Registered SharePoint Sites** tab to configure the Agent type for your SharePoint Online environment. The products that support SharePoint Online are:

- Granular Backup & Restore
- Administrator
- Content Manager
- Replicator
- Deployment Manager
- Archiver
- eRoom Migration
- File System Migration
- Livelink Migration
- Lotus Notes Migration
- Exchange Public Folder Migration
- Quickr Migration
- EMC Documentum Migration
- SharePoint Migration

Refer to the corresponding user guide of each module for more information.

***Note:** If your DocAve 6 Service Pack 5 is upgraded from DocAve 6 Service Pack 2, under the **On-premises** tab, the **SQL Server Data Manager** checkbox and the **High Availability** checkbox are deselected by default; under the **Registered SharePoint Sites** tab, the **File System Migration** checkbox and the **SharePoint Migration** checkbox are deselected by default. If desired, you can manually select these checkboxes after purchasing the corresponding licenses.

- **Job Restriction** – Limit the maximum number of jobs that are allowed to run simultaneously by this Agent by enabling the **Restrict the simultaneously running job count** option and enter a positive integer into the text box.

  The jobs that exceed the number configured here will be put into a queue to be run at a later time. Priority to run each type of jobs can be set by changing the default value of 10 into a positive integer in the configuration file. The number 1 means the highest priority, the number 2 means the second highest priority, and so on. If the priority is the same for different types of jobs, the earlier the jobs are put into the pool, the earlier it runs the jobs.

  Enable the **time out** function and set a specific time in the configuration file for the jobs in the queue. If the waiting time exceeds the set time, the job will fail.

  ***Note**: **Platform Backup and Restore** does not support the **Job Restriction** function.

- **Temporary Buffer** – Select **Local Path** or **UNC Path** to store the temporary files that are generated when running the jobs of the following products: **Report Center**, **Platform Backup & Restore**, **Granular Backup & Restore**, and **High Availability**.

  - **Local path** – Enter a local path in the **Path** text box.
  - **UNC path** – Enter an UNC path in the **UNC path** text box, and then select a managed account profile from the drop-down list. Then, click the **Validation Test** to verify the specified information.

  ***Note**: The temporary files that are generated when running the jobs are saved in the Agent installation directory by default: *…\AvePoint\DocAve6\Agent\temp.*

Once you finish configuring the agent, click **Save** to save the configurations and return to the **Agent Monitor** interface, or click **Cancel** to return to the **Agent Monitor** interface without saving any changes.

- **Configuration File** – Upload the Agent configuration files to the Manager server and change them for the specified Agents. Select the desired DocAve Agents in **Agent Monitor** and click **Configuration File** on the ribbon to change the configuration file for them. In the pop-up window, click **OK** to confirm the modification action and you will be redirected to the configuration page. Refer to the instructions below to change the configuration file.

  ***Note**: Since modifying the Agent configuration files can be risky, AvePoint does not recommend modifying the files.

  - **Agent Information** – View the previously selected Agents.
  - **Browse Configuration File** – Upload the configuration file to the Manager server. Click **Browse** to find the specified **.config** file and click **Open** to upload it. You are able to upload multiple configuration files.

***Note:** The name of the configuration file you upload must have the same name as the existing one, and then you are able to apply the configuration file to destination.

- **Destination Path** – Enter the place where you want to upload the configuration file. DocAve supports configuration file change in **Agent\Bin** and **Agent\data** paths.
- **Conflict Resolution** – Select a resolution when two configuration files have the same name.
  - **Merge** – The content of the newly uploaded configuration file will be merged into the old one.
  - **Replace** – The newly uploaded configuration file will replace the old one.

Click **Save** to change the configuration files as you have configured or click **Cancel** to exit the interface without saving the configuration. If you click **Save**, you will be asked to restart the Agent service. Click **Auto** to automatically restart the Agent service immediately or click **Manual** to manually restart later.

- **View Details** – Click **View Details** on the ribbon to bring up the **View Details** page with information about the selected DocAve Agent. Click the **Summary** tab to view the Agent information. Click the **Agent Types** tab to view all of the Agent types of this selected DocAve Agent.
- **Notification Selection** – Click **Notification Selection** on the ribbon to configure e-mail notification settings. The specified recipients in the selected notification profile will be sent an e-mail when the Agent service is inactive. In the **Notification Selection** page, select a previously configured notification profile from the drop-down menu or select **New Notification Profile** to set up a new e-mail notification profile. For more information about how to configure notification, refer to User Notification Settings.
- **Restart** – Click **Restart** on the ribbon to restart the selected DocAve Agent. This is useful in situations where the Agent is sluggish, or if a job it is running hangs. You can restart the Agent and try again.

  ***Note**: Any jobs that are running against the Agent you are starting may fail.
- **Remove** – Click **Remove** on the ribbon to remove the selected DocAve Agent from **Agent Monitor**. The removed Agent will no longer be used by the Control service. You can only remove Agents that have a down arrow ( ) button in the **Status** column.

  ***Note**: Removing the Agent does not uninstall the Agent.

  ***Note**: If the Agent is currently used by one or more plans, the Agent cannot be removed.
- **Deactivate** – Click **Deactivate** on the ribbon to deactivate the selected DocAve Agent. Once the Agent is deactivated, it is marked as *Inactive,* and will not be used by the

current Control service. However, the deactivated service will still run normally. This is useful when you want to perform maintenance on a specified DocAve Agent.

***Note**: Any jobs that are running against the Agent you are deactivating may fail.

- **Activate** – Click **Activate** on the ribbon to activate the selected DocAve Agent. Once the Agent is activated, it is marked as *Active,* and will be used by the current Control service.

When you are finished viewing and managing your DocAve Agents, click **Close** on the ribbon to close the **Agent Monitor** tab and return to the **Control Panel** main page.

System Options

Use System Options to customize DocAve General Settings and Security Settings:

- **General Settings** – These settings affect DocAve's interface, which include settings for Appearance and SharePoint Farm Settings. This way, you can have DocAve be displayed in the language of your preference, use date and time format that you are comfortable with, insert a custom logo for your reports and e-mail templates, and rename your SharePoint farms so that it is easier for you to recognize them.
- **Security Settings** – These settings affect access to DocAve, which includes settings for System Security Policy and System Password Policy. This way, you have control over the users that are able to access DocAve.

Configuring General Settings

To access **General Settings** for DocAve, in the **Control Panel** interface, click **General Settings** under the **System Options** heading. The following settings can be configured on this page:

- **Language Preference** – Select a language for DocAve to be displayed in, or allow users to utilize a translation engine to have DocAve displayed in the language of the user's browser.
    - **Display … for all users** – Select this option to display DocAve in the language selected here. To change the display language, click the down arrow (▾) button on the drop-down menu, and select your desired language.
    - **Change to the end user browser used language** – Select this option to display DocAve in the language used by the user's browser. Then select a language for DocAve to be displayed in by default in the **If the language does not change successfully, please select to use a default language** drop-down menu. This way, if DocAve does not properly display in the user's browser language, DocAve will be displayed in the language selected here.
- **Date and Time Format** – Set the system location by selecting a location from the **Locale (Location)** drop-down menu. Set the format for all dates and times displayed in DocAve by selecting a date format from the **Date format** drop-down menu, and selecting a time format from the **Time format** drop-down menu.

- **Customize Logo** – Customize the logo for DocAve system reports and e-mail templates. Click **Browse** to find the desired logo file in the pop-up window, select the logo, and then click **Open** to open it. Click **Show Preview** to view the logo in the **Show Preview** area. To hide the **Show Preview** area, click **Hide Preview.**

  Click and drag the logo in the display field to change its placement. Click the zoom in ( ) button to zoom in, the zoom out ( ) button to zoom out, or the reset the settings ( ) button to reset the settings of the new logo. Click the **Restore to Default** button to roll back to the default logo.

- **Farm Name Mapping** – Customize the display names for your farms in DocAve. To find a specific farm, enter the farm name in the search text box, and click the magnifying glass () button to search.

  ***Note:** The search function is not case sensitive. For each farm, enter the desired display name in the corresponding **Display Name** text box.

When you are finished configuring DocAve General Settings, click **Save** to save all changes, and then click **Close** to close the **System Options** interface. If you click **Close** without saving first, any changes you have made will be lost.

Configuring Security Settings

To access **Security Settings** for DocAve, in the **Control Panel** interface, click **Security Settings** under the **System Options** heading. There are two tabs under **Security Settings**, **System Security Policy** and **System Password Policy**.

System Security Policy

In the **System Security Policy** tab, the following options can be configured:

- **Maximum User Session** – Configure the number of simultaneous logons allowed for DocAve. For any new sessions that surpass the designated number, the earliest session will be terminated.
- **Session Timeout** – Configure how long a user can be inactive before being automatically logged off. Enter an integer into the **Logon will expire in:** text box, and then select either **Minute(s)** or **Hour(s)** in the drop-down menu.
- **Failed Logon Limitation** – Enter the maximum number of failed logon attempts allowed in one day. If a specific account fails to provide the correct login information in a single day, it will be locked. To unlock the specified account, refer to the Account Manager section of this guide.

  ***Note**: This setting only affects local users besides the default **Admin** account. Active Directory users and Windows users added in DocAve are not affected by the limitations.

- **Inactive Period** – Configure how long a user can be inactive before the account is automatically disabled. Enter an integer into the **Deactivate the account when the**

inactive period reaches: text box, and then select either **Day(s)** or **Month(s)** in the drop-down menu. Once deactivated, a DocAve administrator must activate the account before the user can log into DocAve.

***Note:** The **Inactive Period** setting does not take effect on users in the Administrators group.

- **Network Security** – Configure the IP addresses to have the desired level of access to DocAve. To access these settings, select the **Enable network security** checkbox, and then select either:
    - **Trusted network** – If selected, only the IP addresses added to this field can access DocAve. To add an IP address as a trusted network, enter the IP address in the **Equals** text box, and then click **Add**. Repeat these steps to add additional IP addresses.
    - **Restricted network** – If selected, the IP addresses added to this field cannot access DocAve. To add an IP address as a restricted network, enter the IP address in the **Equals** text box, and then click **Add**. Repeat these steps to add additional IP addresses.

System Password Policy

In the **System Password Policy** tab, the following options can be configured:

- **Default Password Settings** – Select the rules to be applied on the password after it has been saved. Select **Account is inactive** if you would like to manually activate the account before it can be used.

  If no option is selected in this field, the password does not need to be modified at first login and it will never expire.

  ***Note:** The **Default Password Settings** configured here is a password setting template shared by all of the newly added local users. When adding local users to DocAve Manager, you can choose to use the **Default** password settings or **Customized** password settings for the local users you are about to add. For more information, refer to Adding Users. The **Default Password Settings** will not take effect on the local users that already exist before configuring the **Default Password Settings**.

- **Maximum and Minimum Password Length** – Enter an integer for the maximum and minimum number of characters allowed in a password.
- **Password Rule** – Configure requirements for password.
    - **Minimum number of alpha** – Enter a positive integer, there must be at least the specified number of letters in the password.
    - **Minimum number of numeric** – Enter a positive integer, there must be at least the specified number of numbers in the password.

- **Minimum number of special characters** – Enter a positive integer, there must be at least the specified number of special characters in the password. The special characters include !, @, #, $, %, ^, &, and *.
- **Password cannot contain user ID** – Select this option and the password cannot contain the user's name.
- **Password cannot contain space** – Select this option and the password cannot contain space(s).

- **Password Expiration Warning** – Send out warnings if the password of a user will expire in the specified time period. Set the period by entering a positive integer using the options of **Day(s)** or **Month(s)**. You can choose the forms of the warning by select **Popup message** or **E-mail Notification**.

Viewing Security Information

DocAve 6 uses passphrase to protect the DocAve databases and secure the communication. Before connecting to the DocAve Manager when installing the DocAve Agents, the passphrase must be entered to verify the access.

The passphrase is configured during the Manager's installation. To manage the passphrase, while in the **System Options** tab, click **Security Information** on the ribbon. You can perform the following actions:

- **Back Up** – Click this button to back up the passphrase to the following path: *…\AvePoint\DocAve6\Manager\KeysBak*.

  AvePoint strongly recommends backing up security keys and save the backup in a safe place.

- **Manage Passphrase** – View and modify the passphrase. The following option will be displayed in the **Manage Passphrase** interface.
  - **Modify** – By default, the password cannot be modified. You can click this button to enable the modification of the default password.

    Enter a new passphrase in the corresponding text box and click **Save** to save it.

  ***Note**: Only the users of the **Administrators** group have the permission to modify the passphrase. For details of adding users into the **Administrators** group, refer to the Managing Users section in **Account Manager**.

Authentication and Account Manager

Use **Authentication Manager** and **Account Manager** to customize which users and user groups have access to DocAve. You can set up DocAve to utilize existing methods for authentication such as **Windows Authentication**, **Active Directory integration (AD)** and **Active Directory Federation Services (ADFS) Integration**, **Client Certificate Authentication**, or manually add specific users and set permission levels.

*__Note:__ In order to add specific users in **Account Manager** that authenticates using **Windows Authentication**, **AD authentication, ADFS authentication**, or **Client Certificate Authentication**, you must first set up the authentication integration in **Authentication Manager**.

Authentication Manager

Use **Authentication Manager** to view and manage integrated authentication methods usable by DocAve. This means that DocAve can leverage your pre-existing authentication methods, and customize it for access to DocAve. These authentication methods include:

- **Windows Authentication** – Allows the users to log into DocAve using their Windows Authentication credentials.
- **Local System** – Allows the users to log into DocAve using their DocAve local accounts.
- **AD Integration** – Allows the users to log into DocAve using their Active Directory authentication credentials.
- **ADFS Integration** – Allows the users to access DocAve as long as they have logged into the local machine using their ADFS credentials.
- **Client Certificate Authentication** – Allows the users to access DocAve using Client Certificate Mapping Services.

To access **Authentication Manager** for DocAve, in the **Control Panel** interface, click **Authentication Manager** under the **Authentication Manager** heading.

On the **Authentication Manager** interface, you can select one authentication method, and click **Set as default** in the **Set as default** column to set the specified authentication method as the default authentication method. After setting the authentication method, you can go to **Account Manager** to add users.

Configuring Windows Authentication

To leverage Windows Authentication credentials to access DocAve, complete the following steps:

1. In the **Authentication Manager** interface, click **Windows Authentication** on the ribbon.
2. Select the **Authentication Type** from the drop-down menu:
    a. NTLM
    b. Negotiate (Kerberos)

    ***Note**: Kerberos authentication method must be previously configured in the operating system before you select the **Negotiate (Kerberos)** option when enabling the integration with **Windows Authentication**. Otherwise, the **NTLM** authentication method will be enabled.

3. Click **Save** to save the changes and close the **Windows Authentication** interface, or click **Back** to close the **Windows Authentication** interface without saving any changes.

Configuring AD Integration

To leverage Active Directory authentication credentials to access DocAve, configure your Active Directories in the **AD Integration** interface. To access your Active Directory integration configurations in the **Authentication Manager** interface, click **AD Integration** on the ribbon. In the AD Integration configuration interface, you will see a list of previously configured Active Directories.

To manage your integrated Active Directories, you can perform the following actions:

- **Add** - To add a new Active Directory, click **Add** on the ribbon and enter the full name of the domain or the address of the domain controller in the **Domain** text box. Select a managed account profile from the drop-down list, ensuring that the username is in the **username@domain** format. Note that the selected managed account profile must be a member of the domain you are adding and must be able to log into the domain successfully.

  Click **Validation Test** to see if the values you entered are valid, and then click **Save** to save the configurations for the new Active Directory and return to the **AD Integration** interface.

  ***Note:** If there are any **Frozen** users that belong to the domain you are about to add, a pop-up window appears to inform you to activate these users. If desired, click **OK** to activate them or click **Cancel** to manually activate these users later in **Account Manager**.

- **Edit** – To make changes to an Active Directory, select the Active Directory by selecting the corresponding checkbox, and then click **Edit** on the ribbon. Make the necessary changes, and then click **Save** to save the changes and return to the **AD Integration** interface, or click **Back** to return to the **AD Integration** interface without saving any changes.

  ***Note:** The domain name cannot be edited in the **Domain** text box.

- **Delete** – To delete an Active Directory:

  i. Select the Active Directory by selecting the corresponding checkbox, and then click **Delete** on the ribbon.

  ii. A pop-up window appears to notify you that "**The user(s) associated with the selected domain(s) will be disabled. The user(s) can be enabled only by adding the selected domain(s) again. Are you sure you want to proceed?**".

  - To remove all of the users that are associated with the selected Active Directories from DocAve, select the **Remove all users associated with the selected domain(s)** checkbox.

- If the **Remove all users associated with the selected domain(s)** checkbox is not selected, the status of the users that belongs to this domain will be changed to **Frozen** after this domain is deleted.

  ***Note:** If the last available user in the Administrators group belongs to the domain you are about to delete, this user will not be removed or frozen.

iii. Click **OK** to confirm the deletion, or click **Cancel** to return to the **AD Integration** interface without deleting the selected Active Directories.

iv. If the users cannot be deleted from Manager for some reasons, a pop-up window will appear to inform you the corresponding reasons. Click **OK** to delete the rest of the users or click **Cancel** to not delete the domain.

- **Enable** – Click **Enable** to allow the use of credentials from the corresponding Active Directory to access DocAve.

  ***Note:** If there are any **Frozen** users that belong to the domain you are about to enable, a pop-up window will appear to inform you to activate these users. If desired, click **OK** to activate them or click **Cancel** to manually activate these users later in **Account Manager**.

- **Disable** – Click **Disable** to not allow the use of credentials from the corresponding Active Directory to access DocAve. This option is useful during the maintenance of the Domain Controller machine. You can disable the integration with the domain to be maintained and enable the integration again after the maintenance.

  To disable a domain:

  i. Select the domain you are about to disable, and then click **Disable** on the ribbon.

  ii. A pop-up window appears to notify you that "**The user(s) associated with the selected domain(s) will be disabled. The user(s) can be enabled only by adding the selected domain(s) again. Are you sure you want to proceed?**".

  - To remove all of the users that are associated with the selected Active Directories from DocAve, select the **Remove all users associated with the selected domain(s)** checkbox.
  - If the **Remove all users associated with the selected domain(s)** checkbox is not selected, the status of the users that belongs to this domain will be changed to **Frozen** after this domain is disabled.

***Note:** If the last available user in the Administrators group belongs to the domain you are about to disable, this user will not be removed or frozen.

iii. Click **OK** to confirm the action, or click **Cancel** to return to the **AD Integration** interface.

iv. If the users cannot be deleted from Manager for some reasons, a pop-up window will appear to inform you the corresponding reasons. Click **OK** to delete the rest of the users or click **Cancel** to not disable the domain.

After enabling AD Integration, add one or more domain users in **Account Manager**. When logging into DocAve Manager using the added domain user, you must enter the domain user in the format of domain\username or username@domain.com in the **Login ID** text box on the DocAve login interface.

Configuring ADFS Integration

To leverage Active Directory Federation Services (ADFS) authentication credentials to access DocAve, configure your ADFS integration in the **ADFS Integration** interface. To access your ADFS integration configurations, in the **Authentication Manager** interface, click **ADFS Integration** on the ribbon, and then select **ADFS Integration** in the drop-down menu. You will be brought to the **ADFS Integration Wizard**. To set up ADFS integration, complete the following steps in the wizard:

1. **ADFS Information** – Configure the following general information of the ADFS you want to integrate:
    a. **ADFS Integration Method** – Select **Manually** to configure the settings yourself, or select **Automatically** to get the required information by using a federation metadata trust XML file.
        - **Manually** – Enter the URL of the security token service (STS) in the **ADFS Issuer** text box in the following format:
          https://full qualified domain name/adfs/ls
        - **Automatically** – Enter the URL of the federation metadata trust XML file in the **Federation Metadata Trust** text box in the following format:
          https://full qualified domain name/FederationMetadata/2007-06/FederationMetadata.xml

    b. **Relying Party Identifier** – Enter DocAve's Relying Party Identifier, which must first be configured in ADFS in the **Relying Party Identifier** text box.

    When you are finished configuring the **ADFS Information**, click **Next** to configure the **Security Token Settings**.

2. **Security Token Settings** – Configure the certificates used in the ADFS integration:
    a. **Token-signing** – Complete one of the following actions:

- Click **Select.** A new **Select Certificate** pop-up window will appear for you to select a token-signing certificate to communicate with ADFS. This certificate must be the same as the one configured in ADFS.
- Click **Find Certificate** to search for a desired certificate, and then select a **Find in:** parameter from the drop-down menu, enter the keywords in the **Contains:** text box, select a **Look in field:** parameter from the drop-down menu, and then click **Find Now** to start the search. Click **Stop** to stop the search. Once you have selected your desired certificate, click **OK** to save and exit the Select Certificate interface, or click **Back** to exit the Select Certificate interface without saving selecting a certificate.

***Note**: The certificate selected here must be the same as the one configured in ADFS.

b. **Token-decrypting (optional)** – Complete one of the following actions:

- Click **Select.** A new **Select Certificate** pop-up window appears for you to select a token-decrypting certificate to protect the communication between DocAve and ADFS. This certificate must be the same as the one configured in ADFS.
- Click **Find Certificate** to search for the desired certificate. Select a **Find in:** parameter from the drop-down menu, enter the keywords in the **Contains:** text box, select a **Look in field:** parameter from the drop-down menu, and then click **Find Now** to start the search. Click **Stop** to stop the search. Once you have selected your desired certificate, click **OK** to save and exit the Select Certificate interface, or click **Back** to exit the Select Certificate interface without saving selecting a certificate.

When you are finished configuring the Security Token Settings, click **Next** to configure the Claim Configuration.

3. **Claim Configuration** – Configure the mappings between the Claim Name displayed in DocAve and the Claim Type displayed in ADFS. You can perform the following actions to your claims:
   a. You can change the order of the claims in the Order column of the table. If a user can be identified using several claims, DocAve will use the Claim Name of the first claim listed here as the display name for each respective user.
   b. Click the delete ( ) button to delete the selected claim.
   c. Click **Auto** to have the claim type be specified automatically after you select the claim name from the **Claim Name** drop-down menu. Click **Manu** to add the claims manually. Click **Auto** to switch back to the default option.
4. **Overview** – Review the settings you have configured in the previous steps. To make changes, click **Edit** in the corresponding section, and you will be brought back to that step so you can make changes.

5. **Finish** – Provides you with three options to import the relying party data for DocAve in ADFS (using the **Add Relying Party Trust Wizard**).
    a. **Option 1** – Click the link to import relying party data that is published online from the local network Federation metadata address.
    b. **Option 2** – Click on the link to download the Federation metadata XML file, and then upload the downloaded file to the ADFS server. Follow the wizard to configure other settings.
    c. **Option 3** – Enter the relying party data and the relying party identifier manually in the ADFS configuration wizard.

    In this step, you can also choose to export the current ADFS configuration information to a specified location by clicking **Export** on the ribbon, and then explore to the location you wish to save the XML file to.

Click **Finish** to save your configurations, and return to the Authentication Manager interface, or click **Cancel** to return to the Authentication Manager interface.

Once you have configured an ADFS integration for DocAve, the **Add Federation Trust** option will become available**. Add Federation Trust** allows you to integrate another trusted ADFS with the ADFS you have already configured for DocAve.

To add integration with another trusted ADFS, in the Authentication Manager interface, click **ADFS Integration** on the ribbon, and then select **Add Federation Trust** from the drop-down menu. In the Add Federation Trust interface, enter the following information:

- **Name** – The name entered here will be displayed in the **Server** drop-down menu on the login page. You can select the corresponding name to log on DocAve using the trusted ADFS.
- **URL** – The identifier of the trusted ADFS.

Click **Add** to add the new record, or click the delete ( ) button to delete a selected ADFS trust.

***Note:** There is a known issue in the Authentication Manager. When logging in as added ADFS users, the login fails because the certificate's **Issue To** does not match with the DocAve Manager URL. To prevent or fix this issue, be sure to meet the following requirements:

- Record the DocAve Manager URL in the address bar of the browser which appears after you click the DocAve Manager shortcut.
- When configuring the endpoint's settings in ADFS server, enter the recorded URL as the IP address.
- Make sure the certificate is trusted and verified when visiting DocAve Manager URL.

Configuring Client Certificate Authentication

In the **Authentication Manager** interface, configure **Client Certificate Authentication** in any of the following ways:

- Click **Enable** in the **Action** column of the **Client Certificate Authentication** row to enable the Client Certificate Authentication.
- Click **Disable** to disable this authentication.
- Click **Set as default** to set this authentication as the default.

Account Manager

Use **Account Manager** to view and manage users for DocAve, as well as configure user groups with custom permission levels. You can give specific people, or groups of people your desired level of access to DocAve.

In **Account Manager** you can security trim DocAve users to limit which DocAve module a user is able to access and which farms and registered site collections specific DocAve users can access. Each user can only be added to the **Administrators** group, one or more System groups, or a Tenant group. The same user can only be added in one kind of DocAve group, either Administrators group, System group, Web Application Tenant Group, or Site Collection Tenant Group. To add a user in one kind of DocAve group to another kind of DocAve group, you must remove this user from the previous group, and then add this user to the new group as a new user.

- **Administrators** – Administrators group is the built-in group which cannot be deleted. Users in this group can manage both System groups and Tenant groups, but they cannot see the objects created by the users in the Tenant groups. Users in the Administrators group manage objects owned by the users in the Tenant group by adding another user in the Tenant groups to manage the Tenant group using the newly added user.
- **System** – System group is the user-defined group. Users in this group can view and modify DocAve objects created by any users in the System groups. Due to different specified permission levels, users in this group can view and modify the SharePoint objects of the specified modules in the specified farm.
- **Tenant** – Tenant group includes Web Application Tenant group and Site Collection Tenant group. There are power users and standard users in the Tenant group. A power user must be added when creating the Tenant group. For more information, refer to Security Trimming Users.

*__Note:__ If you would like to leverage authentication credentials from Windows Authentication, AD, ADFS, or Client Certificate Authentication, you must first configure the relevant integration settings in Authentication Manager.

To access **Account Manager** for DocAve, in the **Control Panel** interface, click **Account Manager** under the **Account Manager** heading. Click **Close** on the ribbon to close the **Account Manager** interface.

Security Trimming Users

If you are using DocAve Governance Automation alongside DocAve 6, it is recommended that you do not have users in the Tenant groups and only use the default System group.

As of DocAve 6 Service Pack 3 and later, DocAve supports security trimming rule to all of the DocAve modules. For details on permission control over the users in the Tenant group and the users in the System group, refer to the information below.

- For users of Administrators group:
    - The users in the Administrators group have the Full Control permission to the whole DocAve platform.
    - The users in the Administrators group cannot directly view the DocAve objects created by the users in the Tenant group. However, the users in the Administrators group can add a user in the Tenant group, and then use the newly added user to view the DocAve objects created by the users in the Tenant group.
    - The built-in administrator **Admin** cannot be deleted. However, it can be deactivated.
    - If the built-in administrator **Admin** is deactivated, you cannot delete or deactivate the last available user in the Administrators group, nor can you change its group by adding it to any System group or Tenant group.
- For users of Tenant group:
    - The users in a Tenant group include power users and standard users.
        - **Power User** – The power users can create and delete any standard users and other power users. The power users can manage all of the objects in their own group. The power users can share the Web applications/site collections and the plans that belong to a standard user to the other standard users.

          *__Note__: The related objects of the deleted standard users or power users will not be deleted. The last power user in the Tenant group cannot be deleted.

        - **Standard User** – The standard user can only have permission to the Web application/site collection when the power user shares the Web application/site collection to him.

          *__Note__: When the power user shares the specified Web applications/site collections to the standard user, the standard user can only view and use the specified Web applications/site collections in the tree, but cannot edit or delete the content of these Web applications/site collections.

***Note:** When logging into DocAve using a standard user in the Tenant group, the standard user cannot perform the **Object-based Restore** jobs in the **Granular Backup & Restore** module.

- The users in the Tenant group cannot view objects created by the users in the Administrators group and System group.
- When a user in the Tenant group is removed from the group, the DocAve plans, profiles, or jobs it creates will not be deleted.
- If there are no plans or data, only users and profiles in the Tenant group you are about to delete, the Tenant group can be deleted. If there are plans and data in the Tenant group you are about to delete, a pop-up window appears to inform you that you cannot delete this tenant group. In this pop-up window, DocAve also provides two workarounds for security reason: one is to manually delete all of the objects in this group, and then delete this group; the other is to remove or disable all of the users in this tenant group to make sure that no users can access this Tenant group.
- The users in the Tenant group can be granted permission to the following modules: **Granular Backup & Restore**, **SharePoint Migration**, **Administrator**, **Content Manager**, and **Replicator**.
- The users in the Tenant group can be granted permission to the following functions in **Control Panel**: **User Notification Settings**, **Security Profile**, **Managed Account Profile**, **Storage Configuration**, **Export Location**, **Mapping Manager**, and **Filter Policy**. For the Web Application Tenant group, power users have permission to the **Account Manager** while standard users do not. For Site Collection Tenant group, power users have permission to the **Account Manager** and **Registered SharePoint Sites** by default while standard users do not.

- For users of System group:
  - Users in a System group can view and modify DocAve plans, profiles, or jobs created by other users in the same group, or in the different System groups. Users in the System group can share data and information. Users in the System group cannot view any plan, profile or job created by a user in the Tenant group.
  - Users in a System group can only see plans, profiles, or jobs of modules they have permission for.
  - Users in a System group only have permission to the DocAve objects associated with the SharePoint objects under the farms where they have permission. Therefore, the users in the System group cannot view or can view but cannot edit the DocAve objects associated with the SharePoint objects under the farms where they do not have permission.
  - If granting permission to users to access a module in the farm, those users in a System group will have permission to access only that selected module for this specific farm.

- If a user in a System group attempts to perform an action upon an object that the user does not have permission to access, a message appears informing the user that there is a permission issue and to contact Administrators for assistance.
- Users in a System group can be granted the permission to all of the DocAve modules.
- Users in a System group can be granted the permission to the following functions in Control Panel: **User Notification Settings**, **Security Profile**, **Registered SharePoint Sites**, **Storage Configuration**, **Export Location**, **Data Manager**, **Index Manager**, **Mapping Manager**, and **Filter Policy**.

- Different users cannot create plans with the same name.
- For security trimming rules of SharePoint Online environment, refer to Registered SharePoint Sites.

Managing Permission Levels

Use **Permission Levels** to create pre-configured permissions that can be applied to user groups. This way you can quickly and easily apply the same permission configuration for multiple users.

To configure permission levels for DocAve, in the **Account Manager** interface, click **Permission Level** on the ribbon. In the **Permission Level** interface, previously configured Permission Levels will be displayed.

To manage your permission levels, you can perform the following actions:

- **Add** – To create a new permission level, click **Add** on the ribbon, and then select **Add System Permission** or **Add Tenant Permission**. The corresponding configuration page appears. Then, you can perform the following actions.
  - **Add System Permission** – Creates system permissions for system groups and users.
    - **Name and Description** – Enter a name for the new system permission level and an optional **Description** for future references.
    - **Module** – Select the modules you want to grant permission to for all groups and users using this permission level.

      For the modules, such as **Granular Backup & Restore**, **Platform Backup & Restore**, **SQL Server Data Manager**, **Report Center**, **Administrator**, and **Deployment Manager**, select the corresponding checkbox to grant

the permission to each function in the corresponding module for all of the groups and users.

***Note:** Selecting **Connector** will grant the groups and users the permission to both the **Connector** module and the **Cloud Connect** module.

- **Add Tenant Permission** – Tenant permission levels are permission settings that can be applied to Tenant groups and users in Tenant groups.
  - **Name and Description** – Enter a name for the new tenant permission level and an optional **Description** for future references.
  - **Module** – Select the modules you want to grant permission to for all groups and users of this permission level.

    For the modules, such as **Granular Backup & Restore**, and **Administrator**, select the corresponding checkbox to grant the permission to each function in the corresponding module for all of the groups and users.

Click **Save** to save the configuration. Click **Cancel** to return to the Permission Level Interface without saving changes. **Edit** – To edit a previously configured permission level, select the permission level you wish to edit by selecting the corresponding checkbox, and then click **Edit** on the ribbon to navigate to the **Edit Permission Level** interface.

- In the **Name and Description** section, you can modify the **Name** and a **Description** of this Permission Level.
- In the **Module** section, you can select the modules or functions you wish to allow this permission level to access by selecting the corresponding checkboxes. You can click on a product suite name to modify the access to its modules, and click the up and down arrows to scroll to product suite tabs that are not currently in view.

  ***Note**: The unlicensed products have grayed out tabs, and cannot be configured.

Click **Save** to save the modifications for the permission level and return to the **Permission Level** interface, or click **Cancel** to return to the **Permission Level** interface without saving the modifications.

***Note:** If the edited permission level is being used, a pop-up window appears to inform you that the permission of the group using this permission level is changed, and the permission of the users in this group is also changed. These permission changes may affect the users' access to the plans or jobs. The changes will take effect from the next login.

- **Delete** – To delete a permission level, select the permission level you wish to delete by selecting the corresponding checkbox, and then click **Delete** on the ribbon. A pop-up window appears to confirm this action. Click **OK** to delete the selected permission level and return to the **Permission Level** interface, or click **Cancel** to return to the **Permission Level** interface without deleting the selected permission level.

  ***Note:** A permission level that is currently being used by one or more groups cannot be deleted.

When you are finished managing your permission levels, click **Cancel** on the ribbon to return to the **Account Manager** interface.

Managing User Groups

User groups allow you to apply the same permission levels to all users within the same user group. This way, you can change the permission levels of multiple users by editing your user group rather than individually configuring permission levels for each user. You can also change the permission levels of a user by changing the group they belong to which has pre-configured permission levels.

To access your user group configurations, in the **Account Manager** interface, click **Groups** on the ribbon. In the Groups configuration interface, you will see a list of previously configured user groups. The **Administrators** group comes pre-configured and users of this group have full control over all modules.

Adding User Groups

To add a new group, click **Add Group** on the ribbon. On the **Add Group** interface, you can perform the following configurations:

Adding a System Group

To add new system groups, refer to the following steps:

1. **Group Name** – Enter a **Group Name** for the new system group, enter an optional **Description** for future references, and then select **System Group** as the group type.
2. Click **Next** to proceed.
3. **Permission** – Configure the **Scope** and **Permission** for this new System group.
   - In the **Where should these permissions be applied?** field, select one of the following options:
     - **Global permission** – Grants the users of this System group access to all farms with the permission levels configured here.
     - **Permission for different farms** – Grants users of this System group access to specific farms with the configured system permission levels.

   ***Note:** You must assign at least one permission level to the new group.

- In the **Which permission levels would you like to grant to the group?** field, select the previously defined system permission levels you want to apply to this group by selecting the corresponding checkboxes. If desired, click each permission level to view or edit the corresponding permission level.

4. Click **Next** to proceed.
5. **Add User** – In the **Which user would you like to add?** field, select users from the drop-down list to add to this System group.
6. Click **Next** to proceed.
7. **Overview** – On the overview page, you can view the group configuration information. Then, choose one of the following options to perform:
    - Click **Finish** to save the configuration;
    - Click **Back** to return to the previous interface;
    - Click **Cancel** to return to the **Account Manager** interface without saving the configurations.

Adding a Tenant Group

To add new tenant groups, complete the following steps:

1. **Group Name** – Enter a **Group Name** for the new Tenant group, and then enter an optional **Description** for future references. Select either of the following two group types.
    - **Web Application Tenant Group** – Tenant group for the Web application level.
    - **Site Collection Tenant Group** – Tenant group for the site collection level.
2. Click **Next** to proceed.
3. **Permission** – In the **Which permission levels would you like to grant to the group?** field, select the previously defined tenant permission levels you want to apply to this group by selecting the corresponding checkboxes. If desired, click each permission level to view or edit the corresponding permission level.

    ***Note:** You must at least assign one permission level to the new group.

4. Click **Next** to proceed.
5. **Scope** – Configure the scope for the permission that you want to grant to the group. The scope configuration is only for the Web Application Tenant groups.
6. **Add User** – In the **Which user would you like to add?** field, select users from the drop-down list to add to this tenant group.
    - **Power User** – Select users as power users to manage this Tenant group and the standard users in this Tenant group. At least one power user should be added to the Tenant group you are about to create.
    - **Standard User** – Optionally select users as the standard users to manage the specified Web applications or site collections.

7. Click **Next** to proceed.
8. **Load Site Collections** – Select the permission to the site collections that an AD user of this group has from the drop-down list if you select the checkbox. This step only appears when you select **Web Application Tenant Group** on the **Group Name** step.
    - **Site Collection Administrator** – It will only display the site collections to which the AD user has **Site Collection Administrator** permission when he browses the tree.
    - **Full Control** – It will only display the site collections to which the AD user has **Full Control** permission when he browses the tree.
    - **Design** – It will only display the site collections to which the AD user has **Design** permission when he browses the tree.
    - **Contribute** – It will only display the site collections to which the AD user has **Contribute** permission when he browses the tree.

    ***Note:** If you select **Full Control** here, it will also display the site collections to which the user has **Site Collection Administrator** permission.

    If you select the permission here, when an AD user of this group browses the tree, it will only display the site collections to which the user has this permission. Otherwise, it will display all of the site collections under the selected Web applications if you leave the checkbox unselected here. More configurations are needed if you select the checkbox here in order to use this function. For more information, refer to the Displaying the Site Collections to Which the User Has Certain Permissions.
9. **Overview** – On the overview page, you can view the group configuration information. Then, select one of the following options to perform:
    - Click **Finish** to save the configuration;
    - Click **Back** to return to the previous interface;
    - Click **Cancel** to return to the **Account Manager** interface without saving the configurations.

Editing User Groups

To edit a group, select the group by selecting the corresponding checkbox, and then click **Edit Group** on the ribbon, or click on the name of the desired group. You will be brought to the **Edit Group** interface. Here you can change the description for this group, as well as the permission scope and permission levels. However, you cannot change the type (System group or Tenant group) of the saved group.

***Note**: If you have a group with **Full Control** permission configured in DocAve 6, after upgrading to DocAve 6 Service Pack 1 or later versions, this group will maintain the **Full Control** permission but this will not display on the interface. When you edit this group and change the permission, a message box pops up to inform you that the **Full Control** permission of this group will be replaced by the newly granted permissions. You can click **OK** to continue the action and save the change or click **Cancel** to

cancel the operation. In DocAve 6 Service Pack 1 or later versions, only users of the **Administrators** group have **Full Control** permission.

When you have finished making changes to the configurations for this group, click **OK** to save and return to the **Account Manager** interface, or click **Cancel** to return to the **Account Manager** interface without saving any changes.

Viewing and Managing Users in User Groups

To view and manage the users in a group, select the group by selecting the corresponding checkbox, and then click **Show Users** on the ribbon. You will be brought to the **Show User(s)** interface. For different types of the groups, the **Show User(s)** interfaces are different.

Viewing and Managing Users in Administrators Group or System Groups

On the **Show User(s)** interfaces of the Administrators group or System groups, you will see a list of all of the users that belong to this group.

You can perform the following actions on the users of this group:

- **Add User to Group** – To add users to this group, click **Add User to Group** on the ribbon. You will be brought to the **Add User to Group** interface. Enter the username of the user you wish to add, and then click the check names ( ) button to verify that the username you entered is valid. Alternatively, you can click the browse ( ) button to search for the desired user. In the pop-up window, enter the value to search for in the **Find** text box, and then click the search ( ) button. Select the desired user. Click **OK** to add the selected user, or click **Cancel** to close the window without adding the user.

  ***Note**: The same user cannot be added to different types of groups.

- **Remove User from Group** – To remove users from this group, select the desired users by selecting the corresponding checkbox, and then click **Remove User from Group** on the ribbon. A confirmation pop-up window will appear to confirm the remove operation. Click **OK** to delete the selected user(s), or click **Cancel** to return to the **Show Users** interface without deleting the users.

Viewing and Managing Users in Tenant Groups

On the **Show User(s)** interface of Web Application Tenant Groups and Site Collection Tenant Groups, you can select different view types of the groups, and perform the following operations:

- **User-based View** – The **Managed Web Applications/Site Collections** and **Plans** will be displayed according to different users. While selecting this view type, the power users and standard users will be displayed on the left pane of this interface. Choose a user by selecting the checkbox beside the user, the **Managed Web Applications/Site Collections** and **Plans** for this specified user will be displayed on the right pane.
  - **Add User** – To add users to this group, click **Add User** on the ribbon. You will be brought to the **Add User** interface. Choose users from the **Select users to add to**

the group drop-down list. Select the user type. Click **Next** to assign the Web applications to the specified users. Click **Next** to assign the plans to the specified users. Click **Next** to go to the **Overview** interface where the **Managed Web Applications**/**Site Collections** and **Plans** assigned to the specified users will be displayed. Click **Finish** to save the configuration.

- **Change Permission** – Changes the permissions of the specified user. When changing the permissions of the specified power user, you have to change it to a standard user first, and then you can change the permission to the site collections, Web applications, and plans. When changing the permissions of the specified standard user, you can change it to a power user. You can also change the permission to the site collections, Web applications, and plans.
- **Remove from Group** – Removes users from this group. Cannot remove the last power user from the Tenant group.
- **Activate** – Activates a selected user.
- **Deactivate** – Deactivates a selected user.
- **Audit Report** – Collects the report for the users in the specified tenant group. For more information, refer to Audit Report.

- **Object-based View** – All the Managed Web Applications/Site Collections and Plans in the group will be displayed. The users who have the permission to the Web applications, site collections, and plans are also displayed here.
  - **Change Permission** – Changes the permissions of the Managed Web Applications/Site Collections and Plans.
  - **Managed Web Applications/Managed Site Collections** – Click the **Managed Web Applications/Managed Site Collections** tab to view all of the managed Web applications or site collections for this Tenant group.
  - **Plans** – Click the **Plans** tab view all of the plans for this Tenant group.

Deleting Groups

To delete a group, select the desired groups by selecting the corresponding checkboxes, and then click **Delete Group** on the ribbon. A confirmation pop-up window will appear to notify you that deleting the group will delete user permissions in the group. Click **OK** to delete the selected groups, or click **Cancel** to return to the **Account Manager** interface without deleting the groups. All users of the group must be removed before the group can be deleted. For more information on how to delete the specific Tenant group, refer to Deleting the Specific Tenant Group.

Displaying the Site Collections to Which the User Has Certain Permissions

When an AD user of a Web application tenant group browses the tree in **Administrator, Content Manager**, **Granular Backup & Restore**, **Replicator**, **SharePoint Migration** modules, it will automatically display only the site collections to which this user has certain permissions. Complete the following steps to use this function.

1. Navigate to **Control Panel** > **Authentication Manager** and enable the **AD Integration** authentication method.
2. Navigate to **AD Integration**> **Add**. The **Add a New Domain** interface appears. Configure the **Domain Information** to add a connection to an Active Directory domain:
    - **Domain** – Enter the name of the domain where the AD users belong in the **Domain** text box.
    - **Specify a managed account profile** – Select a managed account profile from the drop-down list.

    Click **Validation Test** to see if the values you entered are valid, and then click **Save** to save the configurations and return to the **AD Integration** interface. Alternatively click **Cancel** to return to the **AD Integration** interface without saving the configurations.
3. Navigate to **Control Panel** > **Account Manager** and add the Web application tenant group. To add a new group, complete the following steps:
    a. Click **Add Group** on the ribbon. The Add Group interface appears.
    b. On the **Group Name** step of the **Add Group** interface, configure the following settings:
        - **Group Name** – Enter a **Group Name** for the new group, and enter an optional **Description** for future references.
        - **Select a group type** – Select the **Web Application Tenant Group** from the three group types here according to your requirement.

    c. Click **Next** to proceed.
    d. On the **Permission** step, select the previously defined tenant permission levels you want to apply to this group by selecting the corresponding checkboxes.

    ***Note:** You must at least grant one permission level to the new group.

    e. Click **Next** to proceed.
    f. On the **Scope** step, select the Web applications for this group.
    g. Click **Next** to proceed.
    h. On the **Add User** step, select users from the drop-down list to add to this group.
        - **Power User** – Select users as power users to manage this group and the standard users in this group. At least one power user should be added to the group you are about to create.
        - **Standard User** – Optionally select users as the standard users to manage the selected Web applications.

    i. Click **Next** to proceed.
    j. On the **Load Site Collections** step, select the permission to the site collections that an AD user of this group has from the drop-down list after selecting the checkbox.

- **Site Collection Administrator** – It will only display the site collections to which the AD user has **Site Collection Administrator** permission when he browses the tree.
- **Full Control** – It will only display the site collections to which the AD user has **Full Control** permission when he browses the tree.
- **Design** – It will only display the site collections to which the AD user has **Design** permission when he browses the tree.
- **Contribute** – It will only display the site collections to which the AD user has **Contribute** permission when he browses the tree.

***Note:** If you select **Full Control** here, it will also display the site collections to which the user has **Site Collection Administrator** permission.

If you select the permission here, when an AD user of this group browses the tree, it will only display the site collections to which the user has this permission. Otherwise, it will display all of the site collections under the selected Web applications if you leave the checkbox unselected here.

k. Click **Next** to proceed.

l. On the overview page, you can view the group configuration information.

m. Click **Finish** to save the configurations, click **Back** to return to the previous interface, or click **Cancel** to return to the **Account Manager** interface without saving the configurations.

4. Click **Add User** on the ribbon after you return to the **Account Manager** interface. Configure the following settings to add AD users to this Web application tenant group.

- **What kind of user would you like to add?** – Select **Active Directory User/Group** from the drop-down list to utilize the user's active directory authentication credentials for this new user.

  ***Note:** This user type won't appear in the drop-down list without enabling the AD Integration authentication method in **Authentication Manager**.

- **What user would you like to add?** – Enter the name of the user/group you wish to add in the **AD User/Group Name** field, and then click the check names ( ) button to verify that the username you entered is valid. Alternatively, you can click the browse name ( ) button to search for the desired user/group. In the pop-up window, enter the value to search for in the **Find** text box, and then click the find name ( ) button**.** Select the desired user, and then click **Add**. Click **OK** to add the users, or click **Cancel** to close the window without adding the users. Then enter an optional **Description** for future references.

***Note:** If you select **Site Collection Administrator** on the **Load Site Collections** interface, and enter a group name here, the members who belong to this group cannot load the site collections when they browse the tree.

- **To which groups would you like to add the user?** – Set the permissions for this user by adding the user to a previously configured DocAve user group, the user will have all of the permissions of the specified group. Here according to our requirements, select the checkbox beside **Add user to tenant group**. Then, select the Web application tenant group from the drop-down list to add the user.

Click **Save** to save the changes or click **Cancel** to return to the **Account Manager** interface without saving any configurations.

Besides this traditional way to add AD users to the Web application tenant group, we can click **Import in Bulk** on the ribbon in the **Account Manager** interface to import users to the tenant group in bulk.

5. Log into DocAve as an AD user of the Web application tenant group. Select **AD Integration** in the **Log on to** field when you log into like this.
6. Now this function can be used in the **Administrator** module and the **Content Manager** module. For more information, refer to the Administrator User Guide and the Content Manager User Guide.

Audit Report

Audit Report monitors the activities of the DocAve users in the Tenant groups. When users create a plan, delete a profile, install or uninstall Agents, or perform other actions, these actions are logged in the Audit Report. To access **Audit Report**, click **Audit Report** on the ribbon of the **User-Based View** interface.

In the **Audit Report** interface, there are a number of configurable report display settings that you can customize:

- **Range** – Time frame parameter for the report.
- **Frequency** – Time interval the report is displayed in.
- **Type** – Choose to display in **Bar** or in **Line**.
- **Custom** – Customize the time range and frequency in a calendar.
- **Y-Axis** – Set the parameter for the Y-axis.
- **DocAve Auditor** – Activities by time per frequency.
- **Details** – Activities per user with modular data.

You can choose to export the report to a datasheet or export as a screenshot by clicking E**xport to Datasheet** or **Output Screenshot** on the ribbon.

- **Export to Datasheet** – Exports the report to a datasheet. Configure the following settings on the **Export to Datasheet** pop-up window:
    - **Report Format** – Select the desired report format from the drop-down menu.
    - **Date Range** – Select the date range for your report.
    - **Frequency** – Select the frequency for your report time.

  Click **OK** to save your configurations and start to export the report, or click **Cancel** to return to **Audit Report** interface without saving any changes.

- **Output Screenshot** – Export the report as screenshot. After clicking it on the ribbon, a window appears with a preview of the screenshot. Click **Print** to print the screenshot, click **Export** to save the screenshot as an image to your local storage device, or click **Close** once you are done printing or saving the screenshot to close the screenshot preview pop-up window.

Deleting the Specific Tenant Group

The Site Collection Tenant Groups and Web Application Tenant Groups cannot be deleted directly under the following circumstances:

- When the users in the Site Collection Tenant Groups have created plans or added the SharePoint site collections to the SharePoint Sites Groups, this Site Collection Tenant Group cannot be deleted directly.
- When the users in the Web Application Tenant Groups have created plans, this Web Application Tenant Group cannot be deleted directly.

Deleting the Specific Site Collection Tenant Group

If there are site collections in SharePoint Sites group or plans associated with the users in the Site Collection Tenant Group you are about to delete, this group cannot be deleted. There are two solutions for this issue:

- **Solution 1** – Delete all of the site collections and plans (if you want to delete Web Application Tenant Groups, delete all of the plans) that are associated with the users in the Tenant group you are about to delete, and then try to delete this group again. To use this solution to delete the Site Collection Tenant Group, complete the following steps:
    i. Use the power user in the group you are about to delete to log into DocAve Manager, and then delete all of the plans in **Plan Manager** and site collections in the corresponding SharePoint Sites Group associated with the users in this group.
    ii. Use **admin** to log into DocAve Manager.
    iii. Navigate to **Control Panel** > **Account Manager**.

iv. Select the Site Collection Tenant Group you are about to delete, and then click **Delete Group** on the ribbon to delete this group.

- **Solution 2** – Deactivate or delete all of the users in the Site Collection Tenant Group you are about to delete. (You cannot delete the last power user, but you can deactivate it.) This way, any user in this Site Collection Tenant Group cannot log into DocAve Manager. Therefore, all of the data associated with this group is protected. The prompt message will appear to inform the end-users about the issue: **Sorry, the account has been disabled. Please contact the administrator.** To use this solution to delete the Site Collection Tenant Group, complete the following steps:

  i. Use **admin** to log into DocAve Manager.

  ii. Navigate to **Control Panel** > **Account Manager**.

  iii. Select the Site Collection Tenant Group you are about to delete, and then click **Show User(s)** on the ribbon. The **User-Based View** interface appears.

  iv. Click **Deactivate** or **Remove from Group** on the ribbon to deactivate or delete all of the users in this group.

  - If the user you deactivated or deleted is currently using DocAve Manager, a prompt message will appear to inform the end-user about the issue: **Sorry, the current user has been disabled. Please contact the administrator for more information.**
  - When logging into DocAve Manager using the disabled user, the prompt message will appear to inform the end-user about the issue: **Sorry, the current user has been disabled. Please contact the administrator.**

All of the information associated with the group you have deleted is not available. If you want to view or use the site collections or plans associated with the users in the Site Collection Tenant Group, you can activate the corresponding users.

Deleting the Specific Web Application Tenant Group

If there are plans associated with the users in the Web Application Tenant Group you are about to delete, this group cannot be deleted. For more information on solutions for this issue, and the specific steps of the solutions, refer to Deleting the Specific Site Collection Tenant Group.

***Note:** Only deleting all of the plans associated with the users in the Web Application Tenant Group you are about to delete, and then you can delete this Web Application Tenant Group.

Deleting Jobs and Backup Data

If desired, the users in the Tenant groups can delete the jobs and the backup data using the **Delete Job and Backup Data** function in **Job Monitor**.

To delete the jobs and backup data, complete the following steps:

1. Use the power user in the Site Collection Tenant Group to create a plan.

2. Run this newly created plan.
3. Navigate to **Control Panel** > **Account Manager**.
4. Select the Site Collection Tenant Group you are about to delete.
5. Click **Show User(s)** on the ribbon. The **User-Based View** interface appears.
6. Select the standard user.
7. Click **Change Permission** on the ribbon.
8. Share the newly created plan to the standard user. For more information about how to change permission of a standard user, refer to Managing Permission Levels.
9. Use the standard user to log in to DocAve Manager, and then run this newly created plan.
10. Verify the backup data in the storage location.
11. Open **Job Monitor**.
12. Select the job run by the standard user.
13. Select **Delete Job and Backup Data** from the **Delete** drop-down list on the ribbon. The job is successfully deleted from **Job Monitor**.
14. Verify that the backup data is also deleted in the storage location.

For more information, refer to the **Deleting Job and Backup Data** section in DocAve 6 Job Monitor Reference Guide.

Managing Users

***Note**: If a domain is integrated with DocAve and a user from its parent domain, subdomain or trust domain is added in DocAve Account Manager, the corresponding parent domain, subdomain or trust domain will be integrated into DocAve.

To view and manage users, in the **Account Manager** interface, click **Users** on the ribbon. In the **Users** interface, you will see a list of previously added users.

Adding Users

To add a user for DocAve, click **Add User** on the ribbon. You will be brought to the **Add User** interface.

Adding a Local User

In the **Add User** interface, complete the following steps to add a local user:

1. **What kind of user would you like to add?** – Select **Local User** from the drop-down list to manually enter the authentication credentials for this user.
2. **Which user would you like to add?** – Enter the **Username** and **E-mail** of the user you are adding, as well as an optional **Description** for future references.
3. **What security settings would you like to configure for this user?** – Enter the desired password into the **Password** and **Confirm password** text boxes, and then configure the **Password settings**.

The password entered here must meet the **System Password Policy**. For more information, refer to System Password Policy.

You can select to use the **Default** password settings, or select **Customized** to configure the password settings manually; select the corresponding checkbox to enable **User must change password at next logon**, **User cannot change password**, **Password never expires**, **Account is inactive**.

4. **To which groups would you like to add the user?** – Set the permissions for this user by adding the user to a previously configured DocAve user group. The user will have all of the permissions of the specified group:
    - **Do not add to any group** – Select this option if you do not want to add this user to any DocAve groups.
    - **Add the user to administrators group** – Select this option to add user to the Administrators group.
    - **Add user to system groups** – Select one or more System groups from the drop-down list to add the user.
    - **Add user to tenant group** – Select an existing Tenant group from the drop-down list to add the user. A user can only be added to one Tenant group.
5. Click **Save** to save the changes or click **Cancel** to return to the **Account Manager** interface without saving any configurations.

Adding an Active Directory User/Group

Before adding Active Directory user or group to DocAve Manager, make sure the **AD Integration** has been enabled in **Authentication Manager**. Complete the following steps to add an Active Directory user or group:

1. **What kind of user would you like to add?** – Select **Active Directory User/Group** from drop-down list to utilize the user's active directory authentication credentials for this new user.
2. **What user would you like to add?** – Enter the name of the user/group you wish to add into the **AD User/Group Name** field, and then click the check names ( ) button to verify that the username you entered is valid. Then, enter an optional **Description** for future references.

    Alternatively, you can also:

    a. Click the browse name ( ) button to search for the desired user/group.

    b. In the pop-up window, enter the value to search for in the **Find** text box.

    c. Click the find name ( ) button**.**

    d. Select the desired user, and then click **Add**.

    e. Click **OK** to add the users, or click **Cancel** to close the window without adding the users.

3. **To which groups would you like to add the user?** – Set the permissions for this user by adding the user to a previously configured DocAve user group, the user will have all of the permissions of the specified group:
    - **Do not add to any group** – Select this option if you do not want to add this user to any DocAve groups.
    - **Add user to administrators group** – Select this option if you want to add this user to Administrators group.
    - **Add user to system groups** – Select one or more System groups from the drop-down list to add the user.
    - **Add user to tenant group** – Select an existing Tenant group from the drop-down list to add the user. A user can only be added to one Tenant group.
4. Click **Save** to save the changes or click **Cancel** to return to the **Account Manager** interface without saving any configurations.

Adding a Windows User/Group

Before adding Windows user or group to DocAve Manager, make sure the **Windows Authentication** has been enabled in **Authentication Manager**. To add a Windows user/group, complete the following steps:

1. **What kind of user would you like to add?** – Select **Windows User/Group** from the drop-down list to utilize the user's Windows authentication credentials for this new user.
2. **Which user would you like to add?** – Enter the username of the user/group you wish to add into the **Windows User/Group Name** field, and then click the check names ( ) button to verify that the username you entered is valid. The users/groups who are in the same domain as the DocAve Control server can be added to DocAve. Then, enter an optional **Description** for future references.

    Alternatively, you can also:

    a. Click the browse name ( ) button to search for the desired user/group.

    b. In the pop-up window, enter the value to search for in the **Find** text box.

    c. Click the find name ( ) button**.**

    d. Select the desired user, and then click **Add**.

    e. Click **OK** to add the users, or click **Cancel** to close the window without adding the users.

    ***Note**: In order to log into DocAve Manager using the added user, the corresponding user must have the permission to access the machine where the DocAve Control service is installed.

3. **To which groups would you like to add the user?** – Set the permissions for this user by adding the user to a previously configured DocAve user group, the user will have all of the permissions of the specified group:

- **Do not add to any group** – Select this option if you do not want to add this user to any DocAve groups.
- **Add user to administrators group** – Select this option if you want to add this user to Administrators group.
- **Add user to system groups** – Select one or more System groups from the drop-down list to add the user.
- **Add user to tenant group** – Select an existing Tenant group from the drop-down list to add the user. A user can only be added to one Tenant group.

4. Click **Save** to save the changes or click **Cancel** to return to the **Account Manager** interface without saving any configurations.

Adding an ADFS Claim User

Before adding ADFS Claim user or group to DocAve Manager, make sure the **ADFS Integration** has been enabled in **Authentication Manager**. Complete the following steps to add an ADFS Claim user:

1. **What kind of user would you like to add?** – Select **ADFS Claim** from the drop-down list to utilize the user's ADFS authentication credentials for this new user.
2. **Which user would you like to add?** – Select a **Claim name** from the drop-down menu. Claims are configured in **Authentication Manager**. Enter the username in the **Claim value** text box. The value entered in the **Claim value** text box will be displayed as the login name for the user in DocAve.
3. **To which groups would you like to add the user?** – Set the permissions for this user by adding the user to a previously configured DocAve user group, the user will have all of the permissions of the specified group:
    - **Do not add to any group** – Select this option if you do not want to add this user to any DocAve groups.
    - **Add user to administrators group** – Select this option if you want to add this user to the Administrators group.
    - **Add user to system groups** – Select one or more system groups from the drop-down list to add the user.
    - **Add user to tenant group** – Select an existing tenant group from the drop-down list to add the user. A user can only be added to one tenant group.

    ***Note:** When using an ADFS Claim user who belongs to different types of DocAve groups to log into DocAve Manger, this ADFS Claim user cannot check which group it belongs to; therefore, it cannot select which role (the group permission) it want to use to log in to DocAve Manager.
4. Click **Save** to save the changes or click **Cancel** to return to the **Account Manager** interface without saving any configurations.

Adding a Client Certificate User

Before adding Client Certificate user to DocAve Manager, make sure the **Client Certificate Authentication** has been enabled in **Authentication Manager**. Complete the following steps to add a Client Certificate user:

1. **What kind of user would you like to add?** – Select **Client Certificate User** from the drop-down list to utilize the user's Client Certificate authentication credentials for this new user.
2. **Which user would you like to add?** – Enter the username of the user/group you wish to add into the **Windows User/Group Name** field, and then click the check names ( ) button to verify that the username you entered is valid. The users/groups in the same domain as the DocAve Control server can be added to DocAve. Then, enter an optional **Description** for future references.

   Alternatively, you can also:

   a. Click the browse name ( ) button to search for the desired user/group.

   b. In the pop-up window, enter the value to search for in the **Find** text box.

   c. Click the find name ( ) button**.**

   d. Select the desired user, and then click **Add**.

   e. Click **OK** to add the users, or click **Cancel** to close the window without adding the users.

   ***Note**: In order to log into DocAve Manager using the added user, the corresponding user must have the permission to access the machine where the DocAve Control service is installed.

3. **To which groups would you like to add the user?** – Set the permissions for this user by adding the user to a previously configured DocAve user group, the user will have all of the permissions of the specified group:

   - **Do not add to any group** – Select this option if you do not want to add this user to any DocAve groups.
   - **Add user to administrators group** – Select this option if you want to add this user to the Administrators group.
   - **Add user to system groups** – Select one or more System groups from the drop-down list to add the user.
   - **Add user to tenant group** – Select an existing Tenant group from the drop-down list to add the user. A user can only be added to one Tenant group.

4. Click **Save** to save the changes or click **Cancel** to return to the **Account Manager** interface without saving any configurations.

After successfully add the client certificate user, you can log into DocAve Manager using the newly added client certificate user. When logging into DocAve Manager, complete the following steps:

1. Open the DocAve Manager login interface.
2. Select **Client Certificate** from the **Log on to** drop-down list.

3. Click **Login**. A pop-up window appears to let you select the certificate.
4. Select a desired certificate and then click **OK**. You are logging into DocAve Manager using the corresponding client certificate user.

Importing AD Users in Bulk

We can use this function to import AD users in bulk, which is a more efficient way to add AD users to system groups and tenant groups.

- Navigate to **Control Panel**> **Account Manager**> **Import in Bulk**, the **Import in Bulk** interface appears.
- Click **Download Template** on the ribbon to download a template for importing users to the system group or tenant group.
- Enter the username, group name and select the user type in the template if you are about to add users to a tenant group, or enter the username and group name in the template if you are about to add users to a system group.

  There are some requirements when you enter values in the tenant group template:

  - Leave no username, group name or user type unspecified when the other one or two columns are specified in the same line.
  - The username you entered must exist in the domain where AD users belong.
  - The same user cannot appear twice in the configuration file.
  - You cannot add users to a tenant group if the username already exists in a DocAve group.
  - The group name you entered must exist in DocAve. It will not create a new group automatically in DocAve if the group name you entered does not exist at all.

  There are some different requirements when you enter values in the system group template:

  - The same user can appear more than once in the configuration file, as long as the corresponding group names are not the same.
  - You cannot add users to a system group if the username already exists in a tenant group or the Administrators group.
- Click **Browse** and upload the configuration file. It will fail to import the users to groups for some reasons after you click **Save** on the ribbon. A message box will pop up or there will be a message displayed on the interface when the following situations occur.
  - There is something wrong with the values you entered. You must obey the rules listed above when you enter the values.
  - The configuration file is open in another program.
  - The AD Integration authentication method is disabled.

- The file format is invalid.
- The file cannot be read properly.
- Try to import users to the tenant group by using the system template or vice versa.

***Note:** A message box pops up if there are some incorrect values. The users shown in the message box cannot be imported to the specified groups, while the other users in the same configuration file can be imported successfully.

***Note:** Users cannot be imported in bulk to the Administrators group.

Viewing User Details

To view a user for DocAve, select the user by selecting the corresponding checkbox, and then click **View Details** on the ribbon. The **View Details** interface appears, where you can view detailed information about the selected user.

Click **Edit User** on the ribbon to edit the user, click **Delete User** on the ribbon to delete this user, click **Activate** to activate this user, click **Deactivate** to deactivate this user, or click **Close** to return to the **Users** interface.

Editing Users

To edit a user for DocAve, select the user by selecting the corresponding checkbox, and then click **Edit User** on the ribbon, or click on the username. The **Edit User** interface appears. Here you can configure the following settings for a user:

1. **What information would you like to edit?** – Edit the user information for the current user.
   - **E-mail** – Enter the e-mail address of the current logged-on user.
   - **Description** – Enter the optional description for future reference.
2. **What security settings would you like to configure for this user?** – Change the user password and configure the security settings for the logged-on user. Select the **Change my password** checkbox. Supply the **New password** and re-enter the new password in the **Confirm new password** field. Select the desired security settings by selecting the corresponding checkboxes. This setting is only for the local users.
   - **User must change password at next logon** – When selecting this option, the specified user must change the password when logging in DocAve next time.
   - **User cannot change password** – When selecting this option, the specified user cannot change the password.
   - **Account is inactive** – When selecting this option, this user account will be inactive.

   Select a deactivation method for the password:
   - **Never** – The password never expires.

- **After __ day(s)** – Enter the number of days you wish the password to be valid for before it expires.
- **On __** – Click the calendar () button to choose the date when you wish the password to expire.

3. **To which group would you like to add the selected user?** – Change the group the logged-on user belongs to. Select the **Add user to administrators group** radio button to add the user to the Administrators group, or select the desired System or Tenant groups from the **Add user to System group(s)** or **Add user to a tenant group** drop-down menu. The user will have all of the permissions of the specified group. Note that you are only able to add/move a user to another group of the same type.

   ***Note**: The **To which group would you like to add the selected user?** field is only used for editing the users in a System group or the Administrators group, or the users who are not added to any DocAve groups. When editing the users in the Tenant groups, this field will be hidden.

   When you are finished, click **Save** to save the changes made and return to the **Users** interface, or click **Cancel** to return to the **Users** interface without saving any changes made.

Deleting Users

To delete a previously configured user, select the users by selecting the corresponding checkboxes, and then click **Delete User** on the ribbon. A confirmation window will pop up for this deletion. Click **OK** to delete the selected users, or click **Cancel** to return to the **Account Manager** interface without deleting the selected users.

Activating and Deactivating Users

Refer to the section below to activate or deactivate a user.

- **Activate** – To activate the **Inactive** user, select the user by selecting the corresponding checkbox, and then click **Activate** on the ribbon.

  ***Note:** If a user fails to provide the correct credentials when attempting to log into DocAve, they will receive the following alert: *Sorry, the login ID or password is incorrect.* If the user receives this alert more times than the number of **Failed Login Attempts** specified in the System Security Policy, the user's account will become **Inactive**.

- **Deactivate –** To deactivate the **Active** user, select the user by selecting the corresponding checkbox, and then click **Deactivate** on the ribbon.

Monitoring Current Logon Accounts

You can view and manage the users currently logged onto DocAve by clicking on **Current Logon Account(s)** on the ribbon of the **Account Manager** interface. This allows you to monitor and control DocAve access in case maximum user sessions limit is met, or if you need to log a user off for security reasons. To log a user off of DocAve, select the user by selecting the correlating checkbox, and then click

Log Off on the ribbon. You will be prompted to enter an optional message to be sent to the user you are logging off. Click **Back** to return to the **Account Manager** interface.

My Settings

In DocAve, some users do not have the permission to navigate to **Account Manager**. **My Settings** allows the user to edit its own Account's information.

- When you log into DocAve GUI, the currently logged-on user will be displayed at the upper-right corner of the DocAve interface. Click the current username, a drop-down list appears. Click **My Settings** and enter **My Settings** interface. In **My Settings** interface, the users in the System groups can view the detailed information of the current logged-on user and the DocAve groups it belongs to; the users in the Tenant groups can view the managed Web applications/site collections and the plans. Click **Edit** on the ribbon and you can configure the settings. For details on how to configure the settings, refer to the Managing Users section in this chapter. Also refer to the detailed information below:
- In the **Password** field, if one user does not have the permission to change the password, the password field will be greyed out. You must supply the **Old password** here.
- The security settings field is greyed out for both the users in the Tenant groups and the user in the System groups.

After you have saved the modifications, click **Close** to exit the **My Settings** interface and return to the previous DocAve interface you are in.

License Manager

License Manager provides you with information regarding your DocAve licenses. Here you are also able to import and export license files, generate license reports, set up expiration notifications, as well as monitor the number of SharePoint servers you have used up in your license.

To access **License Manager** for DocAve, in the **Control Panel** interface, click **License Manager** under the **License Manager** heading. Click **Close** on the ribbon to close the **License Manager** interface.

***Note**: By default, there is a 30-day trial license for all DocAve modules in the downloaded package. This trial license ensures that you can have DocAve up and running right after the Manager and Agent installation completes. To obtain an Enterprise license, contact your local AvePoint representative for details.

Viewing License Information

The **License Manager** interface shows you the following information:

- **License Type** – Shows whether you have a **Trial** license or an **Enterprise** license.

- **Server Host/IP** – Shows the host/IP of the server used to install DocAve Control Service. If the value of this field is N/A, it means that all of the servers where the DocAve Managers reside can use this license.
- **Maintenance Expiration Details** – The expiration date of the DocAve maintenance service you have purchased.
- **License Details** – Display the detailed license information for every module. Note that you are able to view the modules you are licensed for and the modules you have used in the past that occupied some of the total quota.

  Click the tabs **Data Protection**, **Administration**, **Storage Optimization**, **Report Center**, **Compliance**, **Migration**, **Remote Farm**, and **Governance Automation** to see license information specific to that module:

  - **Module** – The name of the DocAve product.
  - **License Type** – The type of license purchased for the product.
  - **Servers in License** – The number of servers you have bought.

    The Number of Servers/VMs – The number of servers/VMs you have bought. (This column only appears under the **Data Protection** tab.)
  - **Servers Registered** – The number of servers you have used.

    Registered Servers/VMs – The number of servers/VMs you have used. (This column only appears under the **Data Protection** tab.)
  - **Expiration Time** – The expiration time of the license for this product.
  - **Status** – The current status of the product which reflects proper licensing.

  Clicking the **Migration** tab will allow you to also view **Remaining Quantity** and **Total Quantity** information, as well as the amount of data that has been migrated for each migration product.

  Remote Farm is for SharePoint Online and only supports the following modules:

  - Administrator
  - Archiver
  - Content Manager
  - Deployment Manager
  - Granular Backup & Restore
  - Replicator
  - Governance Automation

  If you have a Governance Automation Online license, Governance Automation can be viewed under this tab. The number of User Seats can be viewed under the table.

Generating License Reports

Your license information can be exported to a PDF file so that you can save it. To export a license report, click **Export** on the ribbon, and then click **License Report**. Your browser will ask if you would like to open or save the PDF file. Click **Open** to view the file, or **Save** to save it to a designated location.

***Note**: Make sure the **Downloads** settings of the browser are configured before downloading the license file or the license report.

Importing and Exporting License Files

In **License Manager**, you can import a license file to apply that new license. Since all of DocAve products are installed as a single platform, activating any product is as simple as applying the new license file.

To import a license file, click **Import** on the ribbon. In the **Import License** interface, click **Browse**. Find and choose the desired LIC file, and then click **Open**. You will see a summary view of this license. Click **Save** to apply this license, or click **Cancel** to return to the previous page without applying this license.

***Note**: DocAve will automatically log you off in order to use the new license upon logging in again.

Configuring License Renewal Notifications

***Note:** The **License Renewal Notifications** settings will take effect after you apply the **Enterprise** license.

DocAve can be configured to notify you before licenses or maintenance expires. You can set how many days prior to expiration and at what interval you wish to be notified, as well as configure the method of notification to use.

To configure **License Renewal Notifications**, click **Settings** on the ribbon. The **Settings** interface appears. Here you can configure the following settings for **Notification Schedule**:

- **By expiration date** – Configure these settings for notifications for license expiration:
    - Enter a positive integer in the text box and select **Days**, **Weeks**, or **Months** from the drop-down menu of **Remind me starting from __ before license expires for any modules**.
    - Select the **Interval** checkbox to have the reminder repeat at a set interval. Enter a positive integer into the text box and select **Days**, **Weeks**, or **Months** from the drop-down menu.
- **By maintenance expiration date** – Configure these settings for notifications for maintenance expiration:
    - Enter a positive integer into the text box and select **Days**, **Weeks**, or **Months** from the drop-down menu of **Remind me starting from __ before license maintenance expires**.

    - Select the **Interval** checkbox to have the reminder repeat at a set interval. Enter a positive integer into the text box and select **Days**, **Weeks**, or **Months** from the drop-down menu.

- **By number of servers** – Configure these settings for notifications for the number of available servers left for any module.
    - Enter a positive integer into the text box and DocAve will send you a notification when the number of servers left of any module is less than the specified value.
    - Select the **Interval** checkbox to have the reminder repeat at a set interval. Enter a positive integer into the text box and select **Days**, **Weeks**, or **Months** from the drop-down menu.

Configure the following settings for **Notification Method** (Note that you must select at least one of the options in order for **License Renewal Notifications** to work.):

- **Popup message box when you login** – Select this option to have a message box pop-up with a reminder for expiring licenses or maintenance.
- **E-mail notification** – Select this option to be notified of expiring licenses or maintenance by e-mail based on the **Notification Schedule** you configured above. A drop-down menu will appear where you can either select a previously configured **Notification Profile** or you can choose **New Notification Profile** to set up a new e-mail notification profile. For more information on how to configure the notification profile, refer to User Notification Settings.

When you are finished configuring **License Renewal Notification Settings**, click **Save** to save and return to the **License Manager** interface, or click **Cancel** to return to the **License Manager** interface without saving the new configurations.

Configuring SharePoint Server Usage

In **SharePoint Server Usage**, you can view detailed information of all product license registration, register a new farm or remove a previously registered farm.

Click **SharePoint Server Usage** on the ribbon or the server number in the **Registered Servers** column of the **License Details** area to enter the **SharePoint Server Usage** interface. Clicking the number link in the **Registered Servers** will bring you to the **SharePoint Server Usage** interface with only the server usage information for the corresponding.

***Note**: Only **Data Protection**, **Administration**, **Compliance**, **Report Center**, **Storage Optimization**, and **Governance Automation** can be managed in **SharePoint Server Usage**. **VM Backup and Restore**, **Remote Farm** and **Migration** are not registered by server number.

Click on a product suite tab to expand in the left and view all DocAve products you have purchased within that suite. Then select the product to modify its registered farms. You can perform the following actions:

- Register a farm – Select the farm you want to register in the **Unregistered Farm(s)** list and click **Add>>**. The farm will be moved to the **Registered Farm(s)** list.
- Unregister a farm – Select the farm you want to unregister in the **Registered Farm(s)** list and click **<<Remove** button. The farm will be moved to the **Unregistered Farm(s)** list.
- View detailed registering information of a farm – Select the farm from either of the lists above and click **View Details** on the ribbon. This brings you to the **Report Center** interface where you are able to view the SharePoint topology. For more information, refer to the DocAve 6 Report Center User Guide.

***Note:** If the number of servers in the **Registered Farm(s)** list exceeds the number of servers for which the license you have purchased allows, DocAve will not allow you to register more farms and the warning ( ) button will appear left of the module name.

Click **Save** to save the changes or click **Cancel** to cancel the operation, you will then be redirected to the **License Manager** interface.

Update Manager

DocAve Update Manager provides you with information regarding DocAve versions. You can install the updates, view the installation history, and configure update settings. **Update Manager** allows you to update the current version of DocAve or Governance Automation within the DocAve GUI, which will reduce the time and risk of manual update.

Before performing an update:

- If multiple DocAve Control services are installed in the **Windows Network Load Balance** environment, configure the **Storage Location** before you perform the update operation.
- Make sure the SDK and Management Shell files at the DocAve installation path *…\AvePoint\DocAve6\Shell* are not occupied.

To access **Update Manager** for DocAve or Governance Automation, in the **Control Panel** interface, click **Update Manager** under the **Update Manager** heading. Click **Close** on the ribbon to close the **Update Manager** interface.

Configuring Update Settings

In Update Manager, you can configure settings for custom locations to store updates to. To do so, click **Update Settings** on the ribbon. You will be brought to the **Update Settings** interface where you can configure the following settings:

- **Storage Location** – Enters the UNC path where you are about to store the DocAve updates. To utilize this capability, select the **Use the Net Share path as the update storage location** checkbox, enter the **UNC path** into the corresponding text box, and then select a managed account profile from the drop-down list. Note that the UNC path should be entered in the following format:

\\admin-PC\c$\data or **\\admin-PC\shared** folder

Click **Validation Test** to verify the access to the specified path.

If you are changing the storage location to a new one, you can perform the following two actions on the previously stored updates in the old path.

- **Move the uninstalled update(s) to the new location** – All of the uninstalled updates whose versions are higher than the current DocAve version will be moved to the new location. The original update files in the old location will be deleted.
- **Delete the installed update(s)** – All of the stored files of the installed update(s) will be deleted from the old path.

- **Update Port** – Enter the port to use when updating DocAve Control service in the **Update port** text box. The default port is **14007**.

Managing Updates

To manage available updates, click **Manage Updates** on the ribbon. All of the available updates found by manually uploaded will be listed in this page. You can perform the following actions on these updates:

- **View History** – Click **View History** on the ribbon to view a list of previously installed DocAve or Governance Automation updates. Refer to the Reviewing Installation History of Updates for more information.
- **Browse** – Click **Browse** on the ribbon to look for the updates on your local server. Select the desired update, and then click **Open** to load the update file into DocAve. The hotfix will be stored in the UNC path you specified in **Update Settings**. If there is no UNC path configured, the hotfix will be stored under the default path: *…\AvePoint\DocAve6\Manager\Work\patchFolder*.

  ***Note:** For Governance Automation hotfix, you can only use this function to apply new updates.

- **Install** – Click **Install** to install the selected updates. The following options can be configured in the pop-up window.
  - In the **Manager** tab, all of the installed Manager services will be displayed. Select **Install the update for all the managers below** when installing updates for the DocAve Manager services since all of the available Manager services must be updated at the same time.
  - In the **Agent** tab, select the **Install the update for all of the agents below** checkbox to install the update on all of the Agents or select a farm to update all DocAve Agents in that farm.
  - When selecting a Governance Automation update, the **Governance Automation** tab will be displayed. If selecting the Governance Automation service on this tab, the Governance Automation server will be updated.

***Note:** When installing the new update, the dependent version update will also be installed. For example, if your current DocAve version is DocAve 6 Service Pack 1, when you install the update for DocAve 6 Service Pack 2 Cumulative Update 1, then DocAve 6 Service Pack 2 will also be installed.

***Note**: After the installation or update, a message box will pop up and inform you to make a choice. Click **OK** to restart the IIS automatically or click **Cancel** to restart them manually. RBS and the related solutions will not be upgraded automatically if you click **Cancel**. Complete the following steps manually after you click **Cancel**.

i. Upgrade RBS.

ii. Upgrade the related solutions in **Solution Manager**.

iii. Restart the IIS.

The functions related to RBS and the solutions will fail to work without the manual upgrade or restarting the IIS if you click **Cancel** in the message box. For more information about how to upgrade the RBS and solutions, refer to the Storage Manager User Guide and Managing Solutions respectively.

***Note**: Before installing the selected updates, click the link in the prompted message displayed on the right pane to learn more about the selected updates. The message says: **This update contains several changes to the platform that you must be aware of before upgrading. Please see the latest release notes on http: // www.avepoint.com/support/product-updates.**

***Note:** If the hotfix failed to be installed in **Update Manager**, use the **PatchInstallCLI.exe** tool in the hotfix's package to manually install the hotfix. This tool is only included in the hotfix package for DocAve 6 Service Pack 2 or above and the user guide is not included in it. If desired, contact AvePoint Support for the user guide.

- **Delete** – Click **Delete** to delete the selected updates from DocAve. The browsed update files will be deleted at the same time.

Reviewing Installation History of Updates

To review the installation history of your DocAve or Governance Automation updates, click **View History** on the ribbon. You will see a list of all of the previously installed DocAve or Governance Automation updates.

To see more information about an update, select the update by selecting the corresponding checkbox, and then click **View Details** on the ribbon. In the pop-up window, you can perform the following actions:

- **Uninstall** – Click **Uninstall** to uninstall the selected update. The following options can be configured in the pop-up window.

***Note**: Only hotfixes can be uninstalled. Service Packs (SP) and Cumulative Updates (CU) contain important changes between different versions and cannot be uninstalled.

- In the **Manager** tab, all of the installed Manager services will be displayed, select **Uninstall the update from all the managers below** when uninstalling updates from the DocAve Manager services since all of the available manager services must be updated at the same time.
- In the **Agent** tab, select the **Uninstall the update from all of the agents below** checkbox to remove the update from all of the Agents or select a farm to remove the update from all DocAve Agents in that farm.

When you are finished uninstalling the update from the DocAve services, click **Close** to close the pop-up window. Click **Cancel** twice to return to the **Update Manager** interface.

Application Settings

Application Settings in **Control Panel** allows you to customize configurations that affect all products within the DocAve platform.

Agent Groups

Use **Agent Groups** to assign specific Agents for performing certain jobs. This way, you can maintain balanced work load for different Agents, and not have certain Agents perform slower due to poor load distribution.

To access **Agent Groups** for DocAve, in the **Control Panel** interface, click **Agent Groups** under the **Agent Groups** heading. Click **Close** on the ribbon to close the **Agent Group** interface.

If you have several Agents enabled for an Agent type, they will be displayed in different colors in the **Available Agents** table.

Managing Agent Groups

In the **Agent Groups** interface, you will see a list of previously configured Agent groups.

There is a default Agent group for each **On-premises/Registered SharePoint Sites** farm. The default Agent group contains all of the available Agents for each of the modules. All of the Registered SharePoint Sites Agents (both for SharePoint 2010 and SharePoint 2013) can be added to the same Registered SharePoint Sites Agent Group.

The following settings can be configured in the **Agent Groups** interface:

- **Create** – Click **Create** on the ribbon to create a new Agent group. In the **Create** interface, you can configure the following settings:
    - **Agent Group Name** – Enter a name for the new Agent group, and then enter an optional description for future references.
    - **Farm Type** – Choose from two farm types, **On-premises** for SharePoint on-premises farms and **Registered SharePoint Sites** for registered SharePoint sites. Before setting up the Agent group, go to **Agent Monitor** and configure the Agent type. Only the configured Agent type can be selected in **Available Agents** area.
    - **Farm** (Only for SharePoint on-premises farm) – Select the farm where you want to create this new Agent group.
    - **Available Agents** – Available Agents will be displayed in the lower panel. In the **Available Agents** panel, the number of the available Agents will be displayed on the upper left corner above each product suite name, and the available products for each Agent will be colored in blue. Select the desired Agent by selecting the corresponding checkbox, and then click **Add** to add the Agent to

the Agent group. To remove an Agent from the Agent group, select the desired Agent in the **Agent(s) in Group** column by selecting the corresponding checkbox, and then click **Remove**.

When you are finished, click **Save** to save these configurations and return to the **Agent Groups** interface, or click **Back** to return to the **Agent Groups** interface without saving this new Agent group.

- **View Details** – Select an Agent group by selecting the corresponding checkbox, and then click **View Details** on the ribbon to view detailed information about the Agent group.

  In the **View Details** interface, different Agents are marked using different numbers and colors.

  - Click the product suite tabs to view the modules to which each Agent has the corresponding Agent types. If the Agent has the Agent type for a module, the module will be highlighted in the corresponding Agent's color and the module can use this Agent.
  - Hover over the highlighted numbers on the product suite tabs. The detailed information on the Agent the highlighted number represents is displayed.
  - Click **Edit** on the ribbon to make changes to the configurations of this Agent group. Follow the instructions in the next bullet point for editing Agent groups.

- **Edit** – Select an Agent group by selecting the corresponding checkbox, and then click **Edit** on the ribbon to make changes to the configurations of this Agent groups. In the **Edit Agent Group** interface:

  i. **Agent Group Name** – Enter a new Agent group name.

  ii. **Description** – Enter a description for future reference (optional).

  iii. **Farm** – Select the farm where you want to create this Agent group from the **Farm** drop-down menu.

  iv. **Select Agents** – In the **Available Agents** column on the lower panel, the number of the available Agents will be displayed on the top left corner above each product name, and the available products for each Agent will be colored blue. Select the desired Agent by selecting the corresponding checkbox, and then click **Add** to add the Agent to the Agent group. To remove an Agent from the Agent group, select the desired Agent in the **Agent(s) in Group** column by selecting the corresponding checkbox, and then click **Remove**.

  When you are finished, click **Save** to save all changes made to the configurations of this Agent group, click **Save As** to save the new configurations as a new Agent group, or click **Back** to return to the **Agent Groups** interface without saving any changes.

- **Delete** – Select an Agent group by selecting the corresponding checkbox, and then click **Delete** to delete the selected Agent group. A confirmation window will pop up to ask if

you are sure you wish to delete the selected Agent groups. Click **OK** to delete the selected Agent groups, or click **Cancel** to return to the **Agent Groups** interface without deleting the selected Agent groups.

***Note**: Agent group cannot be deleted when:

- There are other Agents in the Agent group you are about to delete. This only applies for **Default Agent Group**.
- There are plans or profiles associated with the Agents in the Agent group you are about to delete. However, when deleting this kind of Agent group, a pop-up window appears to notify you of the plans or profiles that are associated with this Agent group, and the DocAve group the associated users reside.
    - For the Administrators group and System groups, DocAve will only display **System Group** in the table because the users in the Administrators group or System groups can see the DocAve objects belonging to the other users in these two groups.
    - For Tenant groups, DocAve will display **Tenant Group** and the exact group name in the table because the users in the Tenant group can only see the DocAve objects that belong to the user.

  You can delete the plans and profiles first, and then delete this Agent group.

User Notification Settings

Certain DocAve products provide e-mail reports or notifications to provide you with information when a certain triggering event occurs. Currently, DocAve notifications are provided as a pop-up window within DocAve, or as e-mails to designated recipients.

To access **User Notification Settings** for DocAve in the **Control Panel** interface, click **User Notification Settings** under the **User Notification Settings** heading. Click **Close** on the ribbon to close the **User Notification Settings** interface.

Configuring Outgoing E-mail Settings

The outgoing e-mail server must be configured before DocAve can send out e-mail notifications. To configure the **Outgoing e-mail server**, complete the following steps:

1. Select the **Enable Outgoing E-mail Servers Settings** checkbox in order to activate e-mail server settings.
2. **Outgoing e-mail server (SMTP)** – Enter the address of the outgoing e-mail server.
3. **Port** – Enter the SMTP port. The default SMTP port is **25**. For SSL authentication, the default port is **587**.
4. **Sender** – Enter the e-mail address for all DocAve e-mails to be from.
5. **Username on SMTP** – Enter the sender's username on the SMTP server.
6. **Password on SMTP** – Enter the sender's password to log onto the SMTP server.
7. **SSL authentication** – Configure this option according to your E-mail settings.
8. Click the **Validation Test** button to verify the information entered. If the information you entered is verified successfully, a test e-mail will be sent to the sender you configured.

   ***Note:** If you left **Username on SMTP** and **Password on SMTP** empty, meaning you configured SMTP server as **Anonymous**, DocAve will not verify the validation of the entered credential.
9. Click **Save** to save your configurations and click **Close** to exit the interface.

Configuring Notification E-mail Settings

In the **Notification E-Mail Settings** interface, you will see a list of previously configured e-mail notification profiles.

Creating Notification E-mails

The e-mail notification profile allows you to enter e-mail address to receive reports from DocAve plans and services. To create an e-mail notification profile, complete the following steps:

1. **Notification Name** – Enter a name for this e-mail notification profile and an optional **Description** for future references.

2. **Type** – Select a type of report to be generated in the e-mail notification profile.
    a. **Global report** – Global report e-mail notification profiles can be used by modules with notification options available. These profiles will be available for selection when configuring notifications within each module.
    b. **Service report** – Service report e-mail notification profiles are only used for **Manager Monitor** and **Agent Monitor**. The e-mail address you enter in the specified Service report profile will receive e-mail notifications when the DocAve Manager services or Agent services go down.
3. **Notification Address** – Configure the recipients for this notification. Click **Add a Notification Address** and then follow the steps below to add a recipient:
    a. (**Only for Global report**) Choose the detail level for the notification from the drop-down menu in the **Report** column. Select either **Summary Report Recipient** or **Detailed Report Recipient**.
    b. Enter the notification recipient's e-mail address in the **Recipient** column.
    c. Repeat the steps above to add more recipients.
4. **Report Settings** – Select the type of information to include for the report level(s), the recipients of the corresponding report types must exist before you can configure the report level(s):
    a. If **Global Report** was select as the report type, configure the available settings below:
        - **Summary report level(s)** – Set when to send the summary report. Unless manually configured, Success, Failure and Warning are all selected. After the job completed/failed/completed with exception, a summary report will be sent to the recipient. And the job status will be included in the subject of the received e-mail.
        - **Detailed report level(s)** – Set when to send the detailed report. By default, Success, Failure and Warning are all selected. After the job completed/failed/completed with exception, a detailed report will be sent to the recipient. The job status will be included in the subject of the received e-mail.
        - **Send All Logs to Recipient According to Status** – Select what kind of logs will be sent to recipient. You can select **Success**, **Failure** or **Warning**. Failure is selected unless manually configured. The job status will be included in the subject of the received e-mail.
        - **Message format** – Select the format which the message will be delivered in: **HTML** or **Plain text**.
    b. If you select **Service Report** in **Type,** configure the settings below in **Report Setting**.
        - **Send all logs to recipient** – Select **Yes** to send all logs to the recipient when the DocAve Manager services or Agent services go down, or select **No** to avoid sending them.

- **Message format** – Select the format which the message will be delivered in: **HTML** or **Plain text**.

Click **Save** on the ribbon to save the settings, or click **Cancel** to return to the **Notification E-mail Settings** interface without saving the profile.

Managing E-Mail Notifications

To see the configurations of a notification profile, select a notification profile, and then click **View Details** on the ribbon. You will see the configuration details of this notification profile.

To change the configurations for a notification profile, select the notification profile from the list of previously configured notification profiles, and click **Edit** on the ribbon. For more information, refer to Configuring Notification E-mail Settings.

To set a notification profile as the default one, select the notification profile from the list of previously configured notification profiles, and click **Set as Default Profile** on the ribbon. The default notification profile will be selected by default when you build up plans or configure notification settings for the DocAve Manager or Agent services.

To delete a notification profile which is no longer needed, select the notification profile from the list of notification profiles, and click **Delete** on the ribbon. Click **OK** to confirm the deletion, or click **Cancel** to cancel the operation.

Job Manager

Use **Job Manager** in **Control Panel** to customize job pruning and job performance alerts configurations that affect the products in the DocAve platform.

Job Pruning

Use **Job Pruning** to set up pruning rules for the records you are no longer running across your farms. When a job record is pruned, it will be deleted from the **Job Monitor** and the DocAve Control database.

After the **Job Pruning** interface appears, a prompt message displays the schedule configuration information. Click the **Configure Schedule** link to configure the schedules for **Job Pruning**.

***Note:** It is highly recommended to configure a Job Pruning policy if you are running backups frequently. This will ensure your databases does not overload with job data.

In **Job Pruning**, you can configure **Job Pruning Rules** for each DocAve module to retain the desired number of jobs, or jobs within a desired time frame. Once you have configured the **Job Pruning Rule** for a module, you may configure a schedule in the **Settings** tab to have DocAve prune jobs according to the **Job Pruning Rules** at a specified time with a specified notification, or manually run pruning jobs by selecting a module by selecting the corresponding checkbox, and click **Prune Now** on the ribbon to

prune jobs for the selected module based on the **Job Pruning Rules** you have configured for each module.

Job Pruning has **Job Monitor** integrated within the interface. To see the progress of your pruning jobs, click **Job Monitor** on the ribbon. For more information about **Job Monitor**, refer to the DocAve 6 Job Monitor User Guide.

To access **Job Pruning** for DocAve in the **Control Panel** interface, click **Job Pruning** under the **Job Pruning** heading. Click **Save** on the ribbon to save any changes made in **Job Pruning**. Click **Close** on the ribbon to close the **Job Pruning** interface.

Configuring Pruning Rules

In the **Rules** tab, select a DocAve module by selecting the corresponding checkbox, and then click **Configure** on the ribbon, or click on the corresponding **Job Pruning Rule** for a module. The **Configure** interface will open in a pop-up window. The following options can be configured:

- **No Pruning** – Select this option to not prune the job records of this module.

  Depending on the module(s) you are configuring pruning rules for, you will be presented with different options:

  - **Keep the last__ job(s)** – Select this option to keep only the desired number of most recent jobs for this module. Set the number of jobs to keep by entering a positive integer into the text box. For example: If you enter 5 in the text box, only the 5 most recent jobs for this module will be kept. All other job records for this module will be deleted.
  - **Keep the last __ Day(s)/Week(s)/Month(s) of job(s)** – Select this option to keep only the jobs within the desired time frame for this module. Set the time frame for the jobs you want to keep by entering a positive integer into the text box, and then select **Day(s)**, **Week(s)** or **Month(s)** from the drop-down menu. For example: If you enter 7 in the text box, and select Day(s), only jobs performed within the last 7 days by this module will be kept. All the previous job records of this module will be deleted.
  - **Keep the last __ job group(s)** – Select this option to keep only the desired number of most recent job groups for this module. Set the number of job groups to keep by entering a positive integer into the text box. For example: If you enter 5 in the text box, only the 5 most recent job groups for this module will be kept. All other job records for this module will be deleted.
  - **Keep the last __ Day(s)/Week(s)/Month(s) of job group(s)** – Select this option to keep only the job groups within the desired time frame for this module. Set the time frame for the job groups you want to keep by entering a positive integer into the text box, and then select **Day(s)**, **Week(s)** or **Month(s)** from the drop-down menu. For example: If you enter 7 in the text box, and select Day(s), only job groups performed within the last 7 days by this module will be kept. All the previous job records of this module will be deleted.

- **Keep the last __ job(s) or job group(s)** – Select this option to keep only the desired number of most recent jobs/job groups for this module. Set the number of jobs/job groups to keep by entering a positive integer into the text box. For example: If you enter 5 in the text box, only the 5 most recent jobs/job groups for this module will be kept. All other job records for this module will be deleted.
- **Keep the last __ Day(s)/Week(s)/Month(s) of job(s) or job group(s)** – Select this option to keep only the jobs/job groups within the desired time frame for this module. Set the time frame for the jobs/job groups you want to keep by entering a positive integer into the text box, and then select **Day(s)**, **Week(s)** or **Month(s)** from the drop-down menu. For example: If you enter 7 in the text box, and select Day(s), only jobs/job groups performed within the last 7 days by this module will be kept. All the previous job records of this module will be deleted.

When you are finished, click **Save** to save your configurations and return to the **Job Pruning** interface, or click **Cancel** to return to the **Job Pruning** interface without saving any changes.

Configuring Schedule and Notification

Once you have configured **Job Pruning Rules** for DocAve modules, you can set up a schedule for DocAve to run pruning jobs, and notify the designated users with reports about the pruning jobs. In the **Schedule and Notification** tab of the **Job Pruning** interface, configure the following settings:

1. **Schedule Selection** – Set up a schedule for DocAve to run pruning jobs, or select to manually run pruning jobs.
    - **No Schedule** – Select this option if you wish to manually run pruning jobs.
    - **Configure the schedule myself** – Select this option to have DocAve run pruning jobs at a designated time. If this is selected, the **Schedule Settings** configuration will appear. Here you will see a list of all of your previously configured schedules. To add a new schedule, click **Add Schedule**. To edit a previously configured schedule, click on the text in the *Summary* column. To delete a schedule, click the delete ( ) button. To preview the added schedules in a calendar, click **Calendar View**. For more details on adding or editing a schedule, refer to the Configuring a Schedule section of this guide.
2. N**otification** – Select an e-mail notification profile you have previously configured, or click **New Notification** to set up a new e-mail notification profile. For more information about how to configure the notification profile, refer to the User Notification Settings section in this user guide.

Configuring a Schedule

To add or edit a schedule, follow the instructions below:

1. **Type** – Select the time unit of the time interval for this schedule.
    - **By hour** – Configure the schedule by hour

- **By day** – Configure the schedule by day.
- **By week** – Configure the schedule by week.
- **By month** – Configure the schedule by month.

2. **Schedule Settings** – Configure the frequency for this schedule by entering a positive integer in the text box. If you wish to set up a more specific schedule, select the **Advanced** checkbox, more options will appear depending on the **Type** you have selected in step 1:
    - If you selected **By hour**, select one of the following options and configure its settings:
        - **Specify production time**: **From __ to __** – Select the production time, it will run the job pruning in the selected production time frame. Note that all pruning jobs that started within this time frame will finish even if the end time is reached.
        - **Select time below** – Select the time you want to run the job pruning. To add several time points, click **Add**.
    - If you select **By week**, configure the following settings:
        - **Run every __ week(s)** - Enter the frequency in terms of weeks in the text box.
        - **On __** – Select the days of the week to run the job pruning on.
    - If you select **By month**, select one of the following options and configure its settings:
        - **On day __ of __** – Select the day of the specific month(s) to run the pruning jobs. For example, if you select **On day 3 of January** and **July**, the pruning jobs will run on the third of January and July.
        - **Day __ of every __ month(s)** – Select the day of the month and frequency to run the pruning jobs on. For example, if you select **Day 3 of every 3 month(s)**, the pruning jobs will run every three months, on the third of the month.
        - **The __ __of every __ month(s)** – Select on which occurrence of which day(s) of the month, and the frequency to run the pruning jobs. For example, if you select **The First Monday of every 3 month(s)**, the pruning jobs will run every three months, on the first Monday of the month.
        - **The __ __ of __** – Select on which occurrence of which day(s) of which month to run the pruning jobs. For example, if you select **The First Monday of January** and **July**, the pruning jobs will run on the first Monday of January and July.
3. **Range of Recurrence** – Select the **Start time** for pruning jobs. Select one of the following options for the end time and configure its settings:
    - **No end date** – The pruning jobs will run on the configured schedule until you manually end it.
    - **End after __ occurrence(s)** – The pruning jobs will stop running after the number of times you enter here.
    - **End by __** – The pruning jobs will end on the date and time you select here.

4. When you are finished configuring the new schedule you wish to add, click **Save** to save, or click **Cancel** to close the **Add Schedule** interface without saving.

Job Performance Alert

Use **Job Performance Alert** to configure the settings of the job performance alert for the unresponsive jobs for **Administrator**, **Storage Manager**, **Replicator**, **Non-SP Migration**, **Granular Backup & Restore**, **Connector**, **Log Manager**, **Data Manager**, and **Job Pruning**. When a job is not responded for the configured time, a notification e-mail will be sent about this issue.

To access **Job Performance Alert** for DocAve in the **Control Panel** interface, click **Job Performance Alert** under the **Job Manager** heading. Click **Save** on the ribbon to save any changes made in **Job Performance Alert**. Click **Close** on the ribbon to close the **Job Performance Alert** interface.

Configuring Job Performance Alert Settings

To configure the job performance alert for the unresponsive jobs in the **Job Performance Alert** interface, complete the following steps:

1. Select the modules you want to configure the job performance alerts by selecting the corresponding checkboxes.
2. Click **Configure** on the ribbon to configure the job performance alert for the selected modules.
3. In the configure job performance alert interface, the **No alert** radio button is selected by default. Select the **Configure alert settings** radio button to configure the following settings:
    a. **Threshold** – Enter the time period to identify the unresponsive jobs. The entered value should be an integer no less than 30.

       ***Note:** For profiles created before upgrading to DocAve 6 Service Pack 5, if the set value is less than 30, it will change to 30 after the upgrade.

    b. **Actions** – Select at least one action to perform on the unresponsive jobs once they have been identified.

        - **Automatically fail the job** – It will fail the job automatically if the progress has been unresponsive for the minutes that you entered in the **Threshold** field.

          ***Note:** For profiles created before upgrading to DocAve 6 Service Pack 5, this checkbox is selected by default.

        - **Collect the relevant logs for the job** – Select this checkbox to collect the relevant logs for the unresponsive jobs once they have been identified.
        - **Send an e-mail to the addresses configured in the following profile** – Configure to receive a notification e-mail once the unresponsive jobs are identified. You can choose to select a previously configured notification profile from the drop-down list, or click **New Notification** from the drop-down list to create a new

notification profile. Nothing changes if you configure the Report Settings here. The only thing that matters is the addresses configured in the profile.

c. Click **Save** on the ribbon to save the configurations and return to the **Job Performance Alert** interface, or click **Cancel** on the ribbon to return to the **Job Performance Alert** interface without saving changes.

Log Manager

Use **Log Manager** to manage the logs of all of the DocAve services. Logs provide the DocAve support staff with important information for quicker troubleshooting.

Log Manager has **Job Monitor** integrated within the interface. To see the progress of your log collection jobs, click **Job Monitor** on the ribbon. The detailed log collection information will be displayed on the **Job Details** interface. For more information about **Job Monitor**, refer to the DocAve 6 Job Monitor User Guide.

***Note**: A Net Share **Report Location** must be configured in **Job Monitor** before you can use the **Log Manager** when DocAve Control Service Load Balance is used. For more information, refer to the DocAve 6 Job Monitor User Guide.

To access **Log Manager** for DocAve, in the **Control Panel** interface, click **Log Manager** under the **Log Manager** heading. Click **Close** on the ribbon to close the **Log Manager** interface.

Configuring Log Settings

To configure the log settings, in the **Log Manager** interface, click **Log Settings** on the ribbon. You can configure the log settings for the following services by clicking on the corresponding tab:

- Control Service
- Media Service
- Report Service
- Agent

In each of the tabs, you will see the name of the service. For each service, the following options can be configured.

- **Service Host** – The server where the service resides.
- **Log Level** – Logs could be configured to generate on each of the following levels.
    - **Information** (default) – Logs of this level record the basic information of DocAve, such as the jobs that you have ran, the operations you have performed and important processes of jobs. **Information** level logs also contain all of the logs from **Warning** and **Error** levels.

- **Debug** – Logs of this level record the detailed information related to the internal operations such as the communication between DocAve Manager and DocAve Agent, the operations in the database, the output message of the data.

  Logs of this level are used for finding out all of the details of the jobs, and it is recommend that the level is set to **Debug** before troubleshooting. **Debug** level logs also contain all of the logs from **Information**, **Warning**, and **Error** levels.

- **Error** – Logs of this level record the error messages for jobs. Not all of the errors could lead to the failure of the jobs, some of the errors have already been dealt with and the logs will record the detailed information.
- **Warning** – Logs of this level record exceptions for jobs. **Warning** level logs also contain all of the logs from **Error** level.

***Note:** After changing the log levels, the changes will not affect the previous logs but will affect the newly generated logs.

- **Size of Each Log File** –The default size for a log is 5 MB. You can adjust the size according to your requirements by entering a different number into the text box.
- **Total Log File Limit** – The default value is **10**. The maximum number of all of the log files in the **Logs** folder under the installation folder of each Manager service. For each Agent server, the **Total Log File Count** is the maximum number of all of the log files which can be generated by each **.exe** file. The Agent logs are stored in the **Logs** folder under the installation folder of each Agent.

  When the number of log files exceeds the threshold, the oldest log files will be deleted.

When you are finished configuring **Log Settings**, click **Save** to save all changes and return to the **Log Manager** interface, or click **Cancel** to return to the **Log Manager** interface without saving any changes.

You can also configure the log settings in batch by selecting the checkboxes in front of the **Service Name** and clicking **Batch Log Settings** in the ribbon. On the batch settings interface, you can configure the log level, size of each log file, and total log count file.

Scrubbing the Logs

Use **Log Scrub** to scrub the sensitive information in the collected logs. You can configure what kind of information will be replaced and replaced with what kind of information. After you have configured the **Log Scrub Policy**, the collected logs will be displayed according to the configured policy. The sensitive information has been replaced with the configured values in the collected logs.

To scrub the sensitive information in the logs, click **Log Scrub** on the ribbon of the **Log Manager** interface. The **Log Scrub** interface appears.

In the **Log Type** field, the **Collect complete logs** radio button is selected. If you keep this default option, the sensitive information will not be scrubbed in the logs downloaded in **Job Monitor**. To enable the **Log**

Scrub feature, select **Collect logs with sensitive information scrubbed** radio button. The **Log Scrub Policy** field appears. To configure the **Log Scrub Policy**, complete the following steps:

1. Click the **Retrieve Data** link in the **Log Scrub Policy** field or **Retrieve Data** on the ribbon to retrieve the sensitive information from the DocAve databases. The following sensitive information will be retrieved by default.

    - IP address/Hostname
    - Port
    - Username
    - Domain
    - Host Header

    ***Note:** The following sensitive information will not be replaced unless manually configured. Customize the log scrub mappings to replace them.

    - The port used by DocAve Storage Manager and Connector processes to transmit the data required by the enabled EBS/RBS provider. The default value is **14005**.
    - The port used by DocAve Real-time Replicator to inform Replicator processes of the real-time actions captured in SharePoint. The default value is **14006**.
    - The port contained in the SQL Mirroring High Availability job logs and used when creating SQL Mirroring by SQL Server. The default value is **5022**.
    - The IP address of the server where you access DocAve Manager.

    The retrieved sensitive information is displayed in the following two columns in the **Log Scrub Policy** field. If desired, enter the keyword in the search text box to search the information.

    - **Category** – Displays the retrieved sensitive information. Click the desired value to edit it.
    - **Replace with** – Displays the default value with which you are about to replace the sensitive information. Click the desired value to edit it.

      You can adjust how the rows are displayed in the **Log Scrub Policy** field,

        - Select a number from the **Show rows** drop-down list. For example, select **10** from the drop-down list. 10 rows of log scrub mappings are displayed in the **Log Scrub Policy** field.
        - Enter a number in the **Go to _ of _** text box to go to the specified page directly.
        - Click the pervious (<) button to go to the previous page or click the next (>) button to go to the next page.

2. Configure the log scrub policy:

    - **Add** – Enter a sensitive information you are about to replace in the **Category** text box, enter a value with which you are about to replace the specified sensitive information in the **Replace with** text box, and then click **Add** to add it.

- **Delete** – Select one or more log scrub mappings by selecting the corresponding checkboxes, and then click **Delete** to delete this mapping.
- **Export** – Click **Export** on the ribbon to export the log scrub mappings to an .xls file.
- **Import** – After configuring the log scrub mappings in the .xls or .xlsx file, click **Import** on the ribbon to import the configured .xls or .xlsx file. The log scrub mappings in the imported .xls or .xlsx file will be displayed in the **Log Scrub Policy** field.

3. Click **Save** on the ribbon to save the configurations and return to the **Log Manager** interface or click **Cancel** to return to the **Log Manager** interface without saving any changes.

Collecting Logs

In order to collect logs, you must first select the Manager services or Agents that you wish to collect the logs from in the **Log Collection** section of the **Log Manager** interface. Click **Collect** on the ribbon to begin collecting logs for the selected services or agents.

To receive e-mail notification containing the report, select a previously configured e-mail notification profile in the drop-down list or click **New Notification** to set up a new e-mail notification profile. For more information about how to configure the e-mail notification profile, refer to User Notification Settings.

Log Collection Procedure for Trouble Shooting

When some issues occurred during using DocAve products, you can check the logs for more information, and send the collected logs to an AvePoint support if necessary. There are two kinds of ways to collect logs, one is to collect logs through **Log Manager** and **Job Monitor** and the other is to manually copy the log folders.

To collect logs through **Log Manager** and **Job Monitor**, complete the following steps:

1. In the **Log Manager** interface, click **Collect** on the ribbon to collect the logs on the selected services.
2. Click **Job Monitor** to go to **Job Monitor** to view the log collection job.
3. After the log collection job is finished, select the job by selecting the corresponding checkbox.
4. Click **Download**, and then select **Download Job Details** from the drop-down menu.
5. Locate a place to store the downloaded job details.
6. View the collected logs or send the collected logs to an AvePoint support if necessary.

To manually copy the log folders, complete the following steps:

1. Log into the server where DocAve Manager resides.
2. Go to the *...\AvePoint\DocAve6\Manager\Control* directory.
3. Locate the **Logs** folder, and then copy it to a safe place.

4. Go to the …*AvePoint**DocAve6**Manager**Media* directory.
5. Locate the **Logs** folder, and then copy it to a safe place.
6. Go to the …*AvePoint**DocAve6**Manager**Report* directory.
7. Locate the **Logs** folder, and then copy it to a safe place.
8. Log into the server where DocAve Agent resides.
9. Go to the …*AvePoint**DocAve6**Agent* directory.
10. Locate the **Logs** folder, and then copy it to a safe place.
11. View the collected logs or send the collected logs to an AvePoint support if necessary.

In addition, for the users in the **System** and **Administrators** groups, you can also collect the logs of each job by completing the following steps:

1. In the **Job Monitor** interface, select the job whose log you are about to collect by selecting the corresponding text box.
2. Click **Download** on the ribbon, and then select **Download Job Logs**.
3. Go to the directory where the collected logs reside to view the job logs. By default, the logs will be stored in the …*AvePoint**DocAve6**Manager**Work**TempLogFile* directory.
4. View the collected logs or send the collected logs to an AvePoint support if necessary.

For more information, refer to DocAve 6 Job Monitor Reference Guide.

For the users in the Tenant groups, the Agent logs are stored in the separate folders in the …*AvePoint**DocAve6**Agent**Logs* directory by default according to the Tenant groups where the user belongs.

Registered SharePoint Sites

Use **Registered SharePoint Sites** to map out your SharePoint Online/SharePoint on-premises site collections or OneDrive for Business so that you can manage the site collections/OneDrive for Business within those objects with DocAve.

***Note**: There is no need to register SharePoint on premise My Site with the Registered SharePoint Sites.

***Note:** DocAve Agent requires internet access in order for you to add SharePoint Online site collections/ OneDrive for Business to the SharePoint Sites Group/OneDrive for Business Group. For the Agent whose server does not have internet access, you have to configure the **Agent Proxy Settings** before you add SharePoint Online site collections/OneDrive for Business to the SharePoint Sites Group/OneDrive for Business Group. For more information, refer to Agent Proxy Settings.

To access **Registered SharePoint Sites** for DocAve, in the **Control Panel** interface, click **Registered SharePoint Sites** under the **Registered SharePoint Sites** heading. Click **Close** on the ribbon to close the **Registered SharePoint Sites** interface.

Manual Input Mode

Use **Manual Input Mode** to manually add site collections to the SharePoint Sites Group one by one or in bulk using a provided template. You can also use it to manually add OneDrive for Business to the OneDrive for Business Group one by one.

***Note:** The required permissions for the user entered when adding the SharePoint Online site collection/OneDrive for Business to SharePoint Sites Group/OneDrive for Business Group are:

- Site Collection Administrator
- User Profile Service
    - Follow People and Edit Profile
    - Use Tags and Notes
- Managed Metadata Service: Term Store Administrator
- The **Read** permission to the **Apps for SharePoint** library in the app catalog site collection

For more information on the permission requirements to make sure DocAve can use the registered site collection/OneDrive for Business to run each module's job, refer to each module's user guide.

Managing SharePoint Sites Groups/OneDrive for Business Groups

In DocAve's **Registered SharePoint Sites** interface, any SharePoint Sites Groups/OneDrive for Business Groups that you have previously configured will be displayed in the main display pane along with their associated Agent groups, descriptions, and last modified times.

***Note**: The following bullets describe the security trimming for users in the different DocAve groups:

- Users in the System group can also register SharePoint sites/OneDrive for Business to SharePoint Sites Groups/OneDrive for Business Groups, and users within the same System group can view and manage sites created under the same SharePoint Sites Group/OneDrive for Business Group. Users of one System group can also view and modify SharePoint Sites Groups/OneDrive for Business Groups and registered site collections/OneDrive for Business created by users of another System group.
- Users in the Administrators group can view and manage SharePoint Sites Groups/OneDrive for Business Groups and registered site collections/OneDrive for Business created by users of System groups.
- Users in the Site Collection Tenant Group can view and manage only **their own** registered site collections/OneDrive for Business and the corresponding SharePoint Sites Groups/OneDrive for Business Groups where the registered site collections/OneDrive for Business reside, but they cannot view local Farms when managing their site collections/OneDrive for Business using **Granular Backup & Restore**, **Migration**, **Administrator**, **Content Manager**, and **Replicator**.

To manage the SharePoint Sites Groups/OneDrive for Business Groups:

- **Create** – To create a SharePoint Sites Group/OneDrive for Business Group, complete the following steps:

    i. Click **Create** on the ribbon. The **Create** interface appears.

    ii. **SharePoint Sites Group**– Enter a name for this SharePoint Sites Group/OneDrive for Business Group in the **SharePoint Sites Group Name** text box, and then enter an optional description for future reference. Keep in mind that while you are able to enter any name here, AvePoint recommends using names that provide some information as to what type of SharePoint sites/OneDrive for Business should be associated with this group.

    iii. **Group Type** – Choose to create a SharePoint Sites Group or an OneDrive for Business Group.

    iv. **Agent Group** – Select an Agent group to perform DocAve jobs on this SharePoint site/OneDrive for Business. For detailed information on configuring Agent groups, refer to Agent Groups.

    v. Click **Save** to save these configurations and return to the **Registered SharePoint Sites** interface, or click **Cancel** to return to the **Registered SharePoint Sites** interface without saving these configurations.

- **View Details** – Views detailed information of the selected SharePoint Sites Group/OneDrive for Business Group. Select the SharePoint Sites Group/OneDrive for Business Group, and then click **View Details** on the ribbon. The **View Details** interface appears. If desired, click **Edit** on the ribbon to edit the SharePoint Sites Group/OneDrive for Business Group.
- **Edit –** Edits the description for a previously configured SharePoint Sites Group/OneDrive for Business Group. Select the SharePoint Sites Group/OneDrive for Business Group, and then click **Edit** on the ribbon. The **Edit** interface appears.
- **Delete –** Deletes the selected SharePoint Sites Groups/OneDrive for Business Groups. Select the SharePoint Sites Groups/OneDrive for Business Groups, and then click **Delete** on the ribbon.

Managing Site Collections

For each SharePoint Sites Group/OneDrive for Business Group you added to DocAve, you must add one or more site collections/OneDrive for Business to the group in order to manage them with DocAve.

To add site collections/OneDrive for Business to a SharePoint Sites Group/OneDrive for Business Group, select the SharePoint Sites Group/OneDrive for Business Group, and then click **Manage Site Collection** on the ribbon. The **Manage Site Collection** interface appears.

In the **Manage Site Collection** interface for a SharePoint Sites Group/OneDrive for Business Group, you will see a list of previously configured site collections/OneDrive for Business.

- **Add** – Adds a site collection/OneDrive for Business to the specific SharePoint Sites Group/OneDrive for Business Group. Click **Add** on the ribbon. For more information, refer to Adding a SharePoint Site Collection.
- **View Details** – Views the detailed information about a previously added site collection/OneDrive for Business. Select the site collection/OneDrive for Business, and then click **View Details** on the ribbon.
- **Edit –** Edits a previously added site collection/OneDrive for Business. Select the site collection/OneDrive for Business, and then click **Edit** on the ribbon. For more information, refer to Adding a SharePoint Site Collection.
- **Delete –** Deletes a previously added site collection/OneDrive for Business. Select the site collection/OneDrive for Business, and then click **Delete** on the ribbon.
- **Batch Add Site Collections** – Adds site collections to the specific SharePoint Sites Group in bulk. Click **Add Site Collections** on the ribbon. For more information, refer to Adding Site Collections.

  ***Note:** OneDrive for Business cannot be added to the OneDrive for Business Group in bulk.

- **Retrieve Status** – Retrieves the status of the selected site collections/OneDrive for Business. Select the site collections/OneDrive for Business, and then click **Retrieve Status** on the ribbon to retrieve the status of the selected site collections/OneDrive for Business.

Adding a SharePoint Site Collection

To add a site collection, click **Add** on the ribbon. In the **Add a Site Collection** or **Edit a Site Collection** interfaces, configure the following settings:

1. **Site Collection URL** – Enter the URL of the existing site collection you are about to add to this SharePoint Sites Group.

   ***Note:** To use a SharePoint on-premises site collection in the SharePoint Sites Group, if there are Agents on the farm where the site collection resides, make sure the Manager where the site collection is to be registered to has the on-premises license of this farm; if there are no Agents on the farm where the site collection resides, make sure the Manager where the site collection is to be registered to has the Office 365 license.

2. **Site Collection User** – Enter the user who has access to this site collection.
   - **Username** – Enter the username to use in order to manage this site collection.
   - **Password** – Enter the password for the specified account.

***Note:** DocAve does not support to add subsites to the SharePoint Sites Group. If you try to add a subsite to the SharePoint Sites Group, the following two scenarios may occur:

- If the user specified in the **Site Collection User** section does not have permission to the site collection where the subsite you are about to add resides, a pop-up window informs you the site failed to be added to the SharePoint Sites Group, and the current user does not have sufficient permission to the specified site collection.
- If the user specified in the **Site Collection User** section has permission to the site collection where the subsite you are about to add resides, DocAve adds the site collection to the SharePoint Sites Group.

3. Click **Save** to save these configurations and return to the **Manage Site Collection** interface, or click **Cancel** to return to the **Manage Site Collection** interface without saving these configurations.

Adding a OneDrive for Business

To add an OneDrive for Business, click **Add** on the ribbon. In the **Add a Site Collection** or **Edit a Site Collection** interfaces, configure the following settings:

1. In the **How would you like to add the site collection?** field, select a mode.
   - **Add the site collection by entering user information** – Enter the username and password.

     ***Note**: The username used to register the OneDrive for Business can only be used once.

   - **Add the site collection by entering user information and URL** – Enter the site collection URL, username and password.
2. **Site Collection URL** – Enter the URL if **Add the site collection by entering user information and URL** is selected in step 1.
3. **Site Collection User** – Enter the name of the user who has access to the OneDrive for Business and the corresponding password.
   - **Username** – Enter the name of the user who has the OneDrive for Business as My Site if you select the **Add the site collection by entering user information** mode. If you select the **Add the site collection by entering user information and URL** mode, enter the name of the user who has access to the OneDrive for Business
   - **Password** – Enter the corresponding password.
4. Click **Save** to save these configurations and return to the **Manage Site Collection** interface, or click **Cancel** to return to the **Manage Site Collection** interface without saving these configurations.

After clicking **Save**, DocAve will verify the connection between all of the Agents and the entered site collection/OneDrive for Business. If any Agent cannot connect to the entered site collection/OneDrive for Business, a pop-up window appears to inform the end-users that the Agent cannot connect. The window also displays an error message and a suggestion on how to solve the error.

When configuring the site collection/OneDrive for Business, the URL of the site collection/OneDrive for Business will be tested by all of the Agents in the Agent group used by this SharePoint Sites Group/OneDrive for Business Group where the specific site collection/OneDrive for Business resides. Four kinds of icons will be displayed in the **Status** column of the **Manage Site Collection** interface:

- Green check ( ) button – All of the Agents can connect to the specific site collection/OneDrive for Business URL.
- Yellow check ( ) button – Some of the Agents can connect to the specific site collection/OneDrive for Business URL.
- Red X ( ) button – None of the Agents can connect to the specific site collection/OneDrive for Business URL.
- Yellow ! ( ) button – The OneDrive for Business is added into a SharePoint sites group. Besides, this OneDrive for Business is registered before updating to DocAve 6 Service Pack 5, or there is no available Agent when it is being registered.

Unless manually configured, the status of the connection between the Agents and the site collection/OneDrive for Business URL will be checked every 2 hours. The checking frequency can be configured through the configuration file.

Adding Site Collections

You can import the site collections in bulk using the provided template. Click **Batch Add Site Collections** on the ribbon in the **Manage Site Collection** interface to access the **Batch Add Site Collections** interface. To import the site collections, complete the following steps:

1. **Download Template –** Click **Download Template** on the ribbon or click the **download** link to download the configuration file template. Modify the downloaded template to add the site collections' URLs you are about to add to the selected group into the template. Save the modifications and close the modified template.
2. **SharePoint Sites Group** – Displays the name of the selected SharePoint Sites Group.
3. **Upload Configuration File** – Uploads the modified configuration file template. Click **Browse** next to the **File path** text box to upload the modified template.
4. **Site Collection User** – Uses the user specified here to register all of the site collections you are about to add. Enter the **Username** and the corresponding **Password** to access to all of the site collections you are about to import.

   ***Note**: To register SharePoint sites in bulk, the specified user must have the **Design** permission at a minimum to all of the SharePoint sites you are about to add. However, the **Design** permission is not sufficient to use the registered site collections to run jobs. DocAve recommends you use the site administrator who can access all of the site collections you are about to add so that you can normally use the registered SharePoint sites to run jobs.

   ***Note:** If any site collections fail to connect, a pop-up window appears to let you choose to add only the successfully connected site collections, or add all site collections.

5. Click **Save** to save the configurations and return to the **Manage Site Collection** interface.

Scan Mode

Use **Scan Mode** to scan all of the site collections in the specified SharePoint Online admin central site/SharePoint on-premises Web application, or the OneDrive for Business. You can choose to add the discovered site collections/OneDrive for Business to the SharePoint Sites Group/OneDrive for Business Group.

***Note:** If you are using the Agents that have been configured with **Agent Proxy Settings** to scan SharePoint on-premises sites, make sure the proxy server can access the SharePoint on-premises sites you are about to scan.

***Note:** To scan the site collection in the specific SharePoint Web application, make sure the Agent account has the **Full Read** or above permission to this Web application.

***Note:** To scan the site collections in the specific SharePoint admin center site, make sure the Office 365 account has the Global Administrator permission in the specific SharePoint admin center site.

***Note:** To scan the OneDrive for Business, make sure the Agent account has the **Local Administrator** permission to the server where the Agent resides.

Scanning Site Collections

Click **Scan Mode** on the ribbon of the **Registered SharePoint Sites** interface to access the **Scan Mode** interface. To scan the SharePoint Online site collections, OneDrive for Business, or SharePoint on-premises site collections, complete the following steps:

1. Click **Scan** on the ribbon, or click the **Scan** link. A pop-up window appears.
2. Enter the Office 365 account information that will be used to scan all of the site collections in SharePoint Online and OneDrive for Business, or the SharePoint on-premises account information that will be used to scan all of the site collections in the specified Web application.
    - **Use an existing Office 365 account profile** – Use an existing Office 365 account profile to scan the site collections or OneDrive for Business. This radio button is selected by default if there is an existing Office 365 account.
        - **Office 365 Account Profile** – Select an existing Office 365 account profile from the drop-down list.

          ***Note:** If selecting a Global Administrator account and this account is not a site collection administrator, DocAve automatically adds this account to the **Administrators** groups of the site collection or OneDrive for Business.

        - **Scan Scope –** Select to scan SharePoint Online site collections or scan OneDrive for Business.

- **Enter new Office 365 account information** – Configure the Office 365 account that will be used to scan the site collections or OneDrive for Business. This radio button is selected by default if there is no existing Office 365 account.
    - **Office 365 User ID** – Enter the ID of the user that will be used to scan the SharePoint Online site collections or OneDrive for Business.

      ***Note:** If entering a Global Administrator account and this account is not a site collection administrator, DocAve automatically adds this account to the **Administrators** groups of the site collection or OneDrive for Business.

    - **Password** – Enter the corresponding password.
    - **SharePoint Admin Center URL** – The URL of the **SharePoint admin center** site.

      Select the **Save as a new Office 365 account profile** checkbox to save the entered information as a new Office 365 account profile. Once this checkbox is selected, you are required to enter the profile name in the **Profile Name** text box.

    - **Scan Scope –** Select to scan SharePoint Online site collections or scan OneDrive for Business
- **Enter SharePoint account information** – Enter the Web application where you are about to scan and the corresponding SharePoint on-premises credentials.
    - **SharePoint Account** – Enter the SharePoint on-premises account that will be used to connect to the specified Web application. AvePoint recommends you enter a site administrator.

      ***Note:** Only the site collections the specified SharePoint account has permission to will be scanned.

    - **Password** – Enter the corresponding password.
    - **Web Application URL** – Enter the URL of the Web application where you are about to scan.

3. Click **Start** to start to scan the OneDrive for Business, site collections in the specified **SharePoint admin center** or SharePoint on-premises Web application, or click **Cancel** to close the pop-up window without saving any configurations.
4. All of the scanned site collections/OneDrive for Business are displayed in the **Site Collection** column. Select the site collections/OneDrive for Business you are about to add to the specified SharePoint Sites Group/OneDrive for Business Group.

   ***Note:** The displayed site collections/OneDrive for Business in the **Site Collection** table are categorized by farm.

   ***Note:** When selecting SharePoint Sites Group/OneDrive for Business Group, select the checkbox next to the group. One site collection/OneDrive for Business can be added to only one SharePoint Sites Group/OneDrive for Business Group. You can only select one SharePoint Sites

Group/OneDrive for Business Group to add site collections/OneDrive for Business each time. You cannot select multiple SharePoint Sites Groups/OneDrive for Business Groups to add one or more site collections/OneDrive for Business to these groups.

5. For the site collections in the SharePoint Sites Group or the OneDrive for Business in the OneDrive for Business Group, you can perform the following actions:

   - Enter a keyword in the search text box, and then click the search ( ) button to search the desired site collections/OneDrive for Business.

     ***Note:** The search ( ) button can only be used to search site collections/OneDrive for Business. It cannot be used to search SharePoint Sites Group/OneDrive for Business Group.

   - Click **Add** to add the selected site collections/OneDrive for Business to the SharePoint Sites Group/OneDrive for Business Group.
   - Click **Remove** to remove the selected site collections/OneDrive for Business from the SharePoint Sites Group/OneDrive for Business Group.

     ***Note:** Click **Remove** to remove the selected site collections/OneDrive for Business from one SharePoint Sites Group/OneDrive for Business Group, select these site collections/OneDrive for Business in the **Site Collection** table again, and then click **Add** to add these site collections/OneDrive for Business to another SharePoint Sites Group/OneDrive for Business Group.

   Three kinds of icons will be displayed on the right hand of the site collections or OneDrive for Business in the right pane to show the connection status between all of the Agents and the specific site collection/OneDrive for Business URL.

   - Green check ( ) button – All of the Agents can connect to the specific site collection/OneDrive for Business URL.
   - Yellow check ( ) button – Some of the Agents can connect to the specific site collection/OneDrive for Business URL.
   - Reconnect ( ) button – Appears after hovering your mouse over the site collection/ OneDrive for Business if none of the Agents can connect to the specific site collection/OneDrive for Business URL. Click this button to add the site collection/OneDrive for Business to the specific SharePoint Sites Group/OneDrive for Business Group again.

   If there are site collections/OneDrive for Business that failed to be added in the specific SharePoint Sites Group/OneDrive for Business Group, select these site collections/OneDrive for Business, and then click **Reconnect** to add these site collections/OneDrive for Business to the specific SharePoint Sites Group/OneDrive for Business Group again.

6. Click **Save** to save your changes, or click **Cancel** to exit this page without saving any changes.

Adding or Deleting SharePoint Sites Group in Scan Mode

In **Scan Mode**, you can also add a SharePoint Sites Group/OneDrive for Business Group or delete a SharePoint Sites Group/OneDrive for Business Group.

- **New Group** – Creates a new SharePoint Sites Group/OneDrive for Business Group. To do so, click the **New Group** on the ribbon or click the **New Group** link in the **SharePoint Sites Group** box. The **Create SharePoint Sites Group** interface appears. For more information, refer to Managing SharePoint Sites Groups.
- **Delete** – Deletes an existing SharePoint Sites Group/OneDrive for Business Group. Click the **Delete** on the ribbon or click the **Delete** link in the **SharePoint Sites Group** box.

Office 365 Account Profile Manager

Use **Office 365 Account Profile Manager** to manage all of the Office 365 accounts which will be used to scan the OneDrive for Business and all of the site collections on the **SharePoint admin center** site.

To access **Office 365 Account Profile Manager** for DocAve, in the **Control Panel** interface, click **Office 365 Account Profile Manager** under the **Registered SharePoint Sites** heading. Click **Close** on the ribbon to close the **Office 365 Account Profile Manager** interface.

Managing the Office 365 Account Profiles

In the **Office 365 Account Profile Manager** interface, you will see a list of previously configured Office 365 account profiles.

The following settings can be configured in the **Office 365 Account Profile Manager** interface:

- Click **Create** on the ribbon to create a new Office 365 account profile. Configure the following setting:
    i. **Profile Name** – Enter a name for the Office 365 account profile you are about to create.
    ii. **Office 365 Credentials** – Enter the Office 365 credentials for the Office 365 account profile you are about to create.
        - **Office 365 User ID** – Enter the user ID for the Office 365 account profile.
        - **SharePoint Admin Center URL** – Enter the corresponding password for the Office 365 account profile.
    iii. Click **Save** on the ribbon to save your configurations and go back to the **Office 365 Account Profile Manager** interface, or click **Cancel** on the ribbon to go back to the **Office 365 Account Profile Manager** interface without saving any configurations.
- Click **Edit** on the ribbon to edit the selected Office 365 account profile.

i. **Profile Name** – Enter a name for the Office 365 account profile you are about to create.

ii. **Office 365 Credentials** – Enter the Office 365 credentials for the Office 365 account profile you are about to create.

- **Office 365 User ID** – Enter the user ID for the Office 365 account profile.
- **SharePoint Admin Center URL** – Enter the corresponding password for the Office 365 account profile.

iii. Click **Save** on the ribbon to save your configurations and go back to the **Office 365 Account Profile Manager** interface, or click **Cancel** on the ribbon to go back to the **Office 365 Account Profile Manager** interface without saving any configurations.

- Click **Delete** on the ribbon to delete the selected Office 365 account profiles. A prompt message appears to inform you whether or not you want to delete the selected account profiles, click **OK** to delete them or click **Cancel** to go back to the **Office 365 Account Profile Manager** interface.
- Click **Close** on the ribbon to exit the **Office 365 Account Profile Manager** interface and go back to the **Control Panel** interface.

Agent Proxy Settings

Use **Agent Proxy Settings** to configure the proxy settings for the Agents who need to connect to sites outside of these Agents' network, or whose servers do not have internet access and need to communicate to Office 365.

***Note:** If you have configured the **Agent Proxy Settings** in the Agent configuration file, make sure the Agent Proxy Settings configured on the Manager GUI are the same as those in the Agent configuration file. Otherwise, the previous **Agent Proxy Settings** in the Agent configuration file will be overwritten by the settings configured on the Manager GUI.

To access **Agent Proxy Settings** for DocAve, in the **Control Panel** interface, click **Agent Proxy Settings** under the **Registered SharePoint Sites** heading. Click **Close** on the ribbon to close the **Agent Proxy Settings** interface.

Configuring Agent Proxy Settings

In the **Agent Proxy Settings** interface, you will see a list of the available Agents that are registered to the current DocAve Manager. The Agents whose status is down will not be displayed in this interface.

Select one or more Agents, and then click **Proxy Settings** on the ribbon to configure the proxy settings for the selected Agents. The **Proxy Settings** interface appears.

To configure the proxy settings for the selected Agents, complete the following steps:

1. **Proxy Selection** – If you have never configured proxy settings for the selected Agents before, the **No Proxy** radio button is selected in the **Proxy Selection** section by default. If you have configured proxy settings for the selected Agents before, the **HTTP Proxy** is selected by default.
    - Select **No Proxy** to disable the proxy settings for Agents.
    - Select **HTTP Proxy** to configure the proxy settings for Agents. The **Proxy Settings** section appears.
2. **Proxy Settings** – Configure the following proxy settings:
    - **Proxy host** – The hostname or IP address of the proxy server.
    - **Proxy port** – The port used to access the proxy server.
    - **Username** – The username to log into the proxy server.
    - **Password** – The password to access the proxy server.

    ***Note:** The username and password are optional since anonymous proxy is supported.
3. Click **Save** on the ribbon to save your changes and return to the **Agent Proxy Settings** interface, or click **Cancel** to return to the **Agent Proxy Settings** interface without saving any configurations.

Profile Manager

Use **Profile Manager** to manage profiles for application.

Security Profile

Security profile can protect your backup data using the security keys generated by the specified encryption method. Security Profile provides an interface for you to manage DocAve job data security of the following modules: **Granular Backup**, **Platform Backup**, **Content Manager**, **Replicator**, **Archiver**, and **Storage Manager**. In the **Security Profile** pane, there is a default security profile named **Default Security Profile**. It cannot be deleted because it is required for performing data upgrade from DocAve 5 (DocAve 5.7 or later required) or DocAve 6 to DocAve 6 Service Pack 1 or later versions. The default profile is not able to be edited or deleted and only the users in the System groups and Administrators group are able to view it.

Profile Setting

To create a new security profile, click **Create** on the ribbon, and then configure the following settings:

1. **Name** – Enter a profile name and an optional **Description**. When configuring encryption options while creating plans for different DocAve modules, security profile names are listed for you to select from.
2. **Encryption Method** – Select the encryption method and encryption length to be used in the encryption.
    - **Specify an encryption method** – Select an encryption method in the drop-down list from AES, DES and Blowfish. Note that if you are using an FIPS policy in your environment, you can only use AES as the encryption method.
    - **Encryption Length (bit)** – Select the length of the encryption.
3. **Encryption Key** – Select the way to generate an encryption key.
    - **Automatically generate encryption key** – DocAve will generate a randomized key for you.
        - **Update the key every __Years/Months** – Enter an interval to update the key.
    - **Generate encryption key from seed** – Select this option to have DocAve generate a key based on the seed you enter. If you choose this method, enter a seed into the **Seed** text box and then enter the same seed into the **Confirm seed** text box.
4. Click **Save** to save these configurations and return to the **Security Profile** Interface, or click **Cancel** to return to the **Security Profile** interface without saving these configurations. The encryption method or length of a security profile cannot be modified once the profile has been created.

In the **Security Profile** interface, to modify the description and configuration for a previously configured security profile, select the profile you want to modify, and then click **Edit** on the ribbon.

On the **Edit Security Profile** interface, for profiles created in DocAve 6 Service Pack 5, you can click **Update Now** to update the encryption key right away if the **Update the key every _ Months/Years** checkbox is selected, or enter a new seed into the **Seed** text box and the **Confirm seed** text box if **Generate encryption key from seed** is selected. For profiles created before updating to DocAve 6 Service Pack 5, only the name and description can be changed when editing the security profile.

To delete a security profile, select the profile you want to delete, and then click **Delete** on the ribbon.

***Note:** If the security profile you want to delete is already in use, it cannot be deleted.

Importing and Exporting Security Profiles

You can create Security Profiles and export them to be used later. To export the Security Profile, select the profiles you want to export, and click **Export** on the ribbon. You will be asked to create a password for this security profile. Click **OK** after entering the desired password in both the **Password** and the **Confirm password** text boxes. Then click **OK** on the ribbon to save the password and export the profiles to the desired location.

To import the security profile, click **Import** on the ribbon. Enter the password that was created when the profile was exported then click **OK** on the ribbon. The security profile will appear in the list of Security Profiles in the **Security Profile** interface once it has been imported.

To exit the **Profile Manager** interface, click **Close** on the ribbon and return to **Control Panel** interface.

Managed Account Profile

Use **Managed Account Profile** to centralize all of the users used in DocAve Manager.

Security Trimming for Managed Account Profile

The following permissions must be set up for the managed account profile:

- Users in the Administrators group can view and use all of the managed account profiles created by themselves and the users in all of the System groups. However, they cannot view any profiles created by the users in the Tenant groups.
- Users in the System groups can view and use the managed account profiles created by the users in all of the System groups and the Administrators group.
- Users in the Tenant groups can only view and use the managed account profiles created by the users in the same Tenant group. To grant your Tenant group the permission to operate managed account profile, grant your group the permission level with the **Managed Account Profile** checkbox selected.

Managing the Managed Account Profile

In the **Managed Account Profile** interface, you will see a list of previously configured managed account profiles.

***Note:** When you first enter the **Managed Account Profile** interface, there will be one or more managed account profiles in this interface.

The following settings can be configured in the **Managed Account Profile** interface:

- Click **Create** on the ribbon to create a new managed account profile. Configure the following setting:
    i. **Account Credentials** – Enter the account credentials for the managed account profile you are about to create.
        - **Username** – Enter the username for the managed account profile. You can enter the username in the format of **domain\username** or **username@domain.com**.

          ***Note:** DocAve does not support entering **.\Administrator** in this field.
        - **Password** – Enter the corresponding password for the managed account profile.

    ii. Click **Save** on the ribbon to save your configurations and go back to the **Managed Account Profile** interface, or click **Cancel** on the ribbon to go back to the **Managed Account Profile** interface without saving any configurations.

    ***Note:** When using the NetBIOS Name and the Fully Qualified Domain Name (FQDN) of the same user to create managed account profiles, two profiles will be created.

    ***Note:** When using a user in the domain that DocAve Manager cannot recognize to create a managed account profile, DocAve will not validate the entered username and password. However, you can still save this profile. This kind of profile can only be used when entering the credentials for the UNC path.

- Click **View Details** on the ribbon to view the selected managed account profile.
    - **User Name** – The user name in the selected managed account profile.
    - **Modified Time** – The modified time or the selected managed account profile.

    Click **Edit** on the ribbon to edit the selected managed accounts profile, or click **Cancel** to go back to the **Managed Account Profile** interface.
- Click **Edit** on the ribbon to edit the selected managed accounts profile. You can edit the password but not the username. Click **Save** to save your changes and go back to the **Managed Account Profile** interface, or click **Cancel** to go back to the **Managed Account Profile** interface without saving any configurations.

Note: The managed account profile can be saved successfully even if the password is incorrect. While if the managed account profile is being used by one or more modules, it cannot be saved successfully with the incorrect password.

- Click **Delete** on the ribbon to delete the selected managed account profiles. A prompt message appears to inform you whether or not you want to delete the selected account profiles, click **OK** to delete them, or click **Cancel** to go back to the **Managed Account Profile** interface. You cannot delete the managed account profile that DocAve is currently using.
- Click **Close** on the ribbon to exit the **Managed Account Profile** interface and go back to the **Control Panel** interface.

Settings for Specific Products/Modules

Use **Specific Products Settings** to configure settings that may be only relevant to certain products.

Solution Manager

Solution Manager provides an interface for you to manage all of the DocAve solutions. To access **Solution Manager** for DocAve, in the **Control Panel** interface, click **Solution Manager** under the **Solution Manager** heading. Click **Close** on the ribbon to close the **Solution Manager** interface.

*__Note__: To deploy a solution on the SharePoint server, be sure that the Agent account is a member of the local **Administrators** group and the **Farm Administrators** group in the SharePoint server.

*__Note__: If you are using Auditor and want to update DocAve 6 to DocAve 6 Service Pack 1 or later versions, before you update DocAve 6 Auditor data to DocAve 6 Service Pack 1 or later versions, refer to the instruction below to ensure the successful update:

1. Go to SharePoint and delete DocAve 6 solution **SP2010RCAuditorSiteCreationMonitor.wsp**.
2. If you have enabled monitoring Site Deletion action in DocAve 6 Auditor module and want to continue using this function in DocAve 6 Service Pack 1 or later versions , go to the DocAve 6 Agent servers and select the path *…/windows/assembly*, find **SP2010RCAuditorSiteDeletion.dll** and delete it. For detailed information on how to monitor SharePoint actions in DocAve 6 Report Center, refer to the DocAve 6 Report Center User Guide.
3. Go to DocAve 6 Solution Manager and deploy **SP2010AuditorMonitor.wsp** and **SP2010DocumentAuditing.wsp**.

Managing Solutions

When you first access **Solution Manager**, you will see a list of DocAve solutions. In order to see some of the information for these solutions, or to perform certain actions to these solutions, you must first select a farm.

Farm Selection

Select a farm from the **Farm** drop-down menu, the following information of the farm will be displayed in a table:

- **The Number of Front-end Web Servers** – Number of the servers which have enabled the Microsoft SharePoint Foundation Web Application service.
- **The Number of Available Agents** – Number of the DocAve Agents with an up arrow ( ) button and **Active** status.
- **Deployment Method** – Currently the solution can only be locally deployed. In other words, solution files are deployed only to the DocAve Agent server from which the deployment operation was initiated.

Viewing the Solution's Information

View the following information of the solutions in the corresponding table:

- **Solution** – The name of the DocAve solution.
- **Module** – The name of the module this solution is intended for.

The following information is only available if you have a farm selected:

- **Version** – The version of the solution.
- **Status** – The deployment status of the solution file.
  - **N/A** – The solution is not installed.
  - **Not Deployed** – The solution is installed but not deployed.
  - **Deployed** – The solution is deployed to all of the Agent servers.
  - **Partially Deployed** – The solution is deployed to some of the Agent servers.
- **Last Refreshed Time** – The last modified time of the corresponding solution.
- **Message** – Display the detailed information of the solution deployment.

***Note:** The first time you go to **Solution Manager**, it will take you awhile to load all of the available solutions for the selected farm.

Operations on the Solutions

Select a solution from the table by selecting the corresponding checkbox. Perform the following actions as necessary:

***Note**: For the SharePoint 2013 Site Collections with the SharePoint 2010 experience version, you must install and deploy the **Connector**, **Storage Manager**, **Archiver**, and **Report Center** solutions designed for SharePoint 2010.

- **Install** – Click **Install** on the ribbon to add a solution package to the farm's solution store, which is in the farm's configuration database. Use this button when you only want to add the solution to the specified farm and do not want to deploy it.
- **Deploy** – Click **Deploy** on the ribbon to unpack the solution package, and copy its elements to their appropriate places. This button can be used even when the solution has not been installed to the specified farm. In that case, the solution will be installed to the specified farm first and then be deployed.
- **Retract** – Reverse the deployment of the farm solution's components. The solution remains in the solution store and can be redeployed later.
- **Remove** – Deletes the solution package from the solution store. This button can be used even when the solution has not been retracted from the specified farm. In that case, the solution will be retracted from the specified farm first and then be removed.

After a solution is installed, to view information about it, complete the following steps:

1. Select the solution by selecting the corresponding checkbox.
2. Click **Solution Properties** on the ribbon. The **Solution Properties** interface appears. By default, you are in the **Summary** tab, which shows an overall view of the specified solution.
3. Click the **Details** tab to view the solution's deployment status on each of the Web applications and other detailed information.
4. In the **Details** tab, you can also select Web applications by selecting the corresponding checkboxes.
5. Click **Deploy** or **Retract** to deploy or retract the solution from the selected Web applications.
6. When you are finished, click **Back** on the ribbon to return to the **Solution Manager** interface.

Maintaining Solutions

To keep your DocAve solutions up to date, **Solution Manager** provides you tools to check for solution version and upgrade existing solutions. To perform any of these actions, select the solution by selecting the corresponding checkbox, and then click:

- Click **Retrieve Version** on the ribbon to retrieve version information about the selected solutions. The information displayed in the **Version**, **Status**, and **Message** columns will be refreshed.
- Click **Upgrade** on the ribbon to upgrade the selected solution to the latest version. A solution can be upgraded if the solution version is lower than the current Agent version.

Solution Description

Refer to the descriptions below to get an overall view of all of the DocAve 6 solutions.

SharePoint 2010 Solutions

- **SP2010SecurityManagement.wsp** – This solution is only used for the Administrator module for SharePoint 2010 environments. After deploying it, go to SharePoint to active the corresponding features in the specified site collection. You will be able to activate the DocAve Security Management Feature, DocAve Security Management Ribbon, DocAve Security Search History Feature and DocAve Security Search Result Feature. Then you will be able to use the corresponding functions of these features in SharePoint. For more information, refer to the Administrator User Guide.
- **SP2010EndUserGranularRestore.wsp** – This solution is only used for the Granular Backup and Restore module for the SharePoint 2010 environment. After deploying it, navigate to **DocAve Manager** > **Data Protection** > **Granular Backup and Restore** > **Restore** > **End-User Restore**, and select the desired farm, Web application, or site collection where you want to activate this solution. Click **Activate** on the ribbon to activate the solution. You can also go to SharePoint to activate the **End-User Restore for**

SharePoint 2010 feature for each site collection. For more information, refer to the Granular Backup and Restore User Guide.

- **SP2010LotusNotesLinkTracking.wsp** – This solution is used to enhance the DocLinks migration process for SharePoint 2010.
- **SP2010AuditorMonitor.wsp** – This solution is only used for the Report Center module for SharePoint 2010 environments. After deploying it, go to **Report Center** > **Settings** > **Auditor Controller** to activate this feature by selecting the **Site Collection Deletion** or **Site Creation** checkboxes in the **Audit Action** field. For more information, refer to the Report Center User Guide.
- **SP2010DocumentAuditing.wsp** – This solution is only used for the Report Center module for SharePoint 2010 environments. After deploying it, go to **Report Center**> **Settings** > **Manage Features** to activate this feature at site collection level, or go to SharePoint to activate this feature. Then you will be able to audit all documents under the specified site collection and view the auditor history of the documents. For more information, refer to the Report Center User Guide.
- **SP2010UsageActivityWebParts.wsp** – This solution is only used for the Report Center module for SharePoint 2010 environments. After deploying it, you will be able to enable the **AvePoint Social Activity Web Parts** feature at site collection level, allowing you to add Social Activity Web Parts in SharePoint sites. These Web parts display the reports on social activities and contents within a specific farm/Web application/site collection/site. The five Web parts in SharePoint 2010 are Most Active Contributors, Top Documents, Top Blog Posts, Top Discussions, and Top Wiki Pages.

  ***Note:** The Most Popular Contributors Web Part does not support SharePoint 2010.
- **SP2010AlternateFileAccess.wsp** – This solution is used to upload the large files or the files with the file types that cannot be uploaded to SharePoint directly. It is only used for the Storage Manager module for SharePoint 2010 environments. After deploying it, navigate to **Storage Optimization** > **Real-Time Storage Manager** or **Scheduled Storage Manager** > **Manage Feature**, and select the desired farm, Web application, or site collection where you want to activate this solution. Click **Activate** to activate the solution. You can also go to SharePoint to activate the **Alternate File Access** site collection feature for each site collection. For more information, refer to Storage Manager User Guide.
- **SP2010ConnectorContentLibrary.wsp** – This solution is used for the Connector module and the Cloud Connect module in SharePoint 2010 environments. After deploying it, you enable the feature at the site collection level. For more information, refer to the Connector User Guide and the Cloud Connect User Guide.
- **SP2010ConnectorMediaLibrary.wsp** – This solution is used for the Connector module and the Cloud Connect module in SharePoint 2010 environments. After deploying it, you enable the feature at the site collection level. For more information, refer to the Connector User Guide and the Cloud Connect User Guide.
- **SP2010EndUserArchiver.wsp** – This solution is only used for the Archiver module for SharePoint 2010 environments. After deploying it, you are able to use End-User

Archiving in Archiver and the end-users are able to archive data by directly operating on the corresponding objects in SharePoint 2010. For more information, refer to the Archiver User Guide.

- **SP2010ErrorPageforArchivedData.wsp** – This solution is only used for the Archiver module for SharePoint 2010 environments. After deploying it, when an item has been archived and a user want to open the archived item using the original URL, DocAve will check if the item has already been archived, if yes, it will pop up a prompt message. For more information, refer to the Archiver User Guide.
- **SP2010PreviewGUI.wsp –** This solution is used to preview the files in SharePoint. It is only used for the SharePoint 2010 environments. After deploying it, you will be able to enable the corresponding feature at the site collection level, allowing you to preview the files in SharePoint 2010. For more information, refer to the Connector User Guide.
- **SP2010StorageManagerStubTraceManagement.wsp –** This solution is used to show the externalized details for the documents and attachments in SharePoint 2010. After the solution is deployed, navigate to **Storage Optimization** > **Real-Time Storage Manager** or **Scheduled Storage Manager** > **Manage Feature** > **Stub Trace**. Click **Activate All** to activate the **Stub Tracing** feature on all of the site collections in the selected Web application, or click **Activate** to activate the **Stub Tracing** feature on the selected site collection. For more information, refer to DocAve Storage Manager User Guide.

SharePoint 2013 Solutions

- **SP2013SecurityManagement.wsp** – This solution is only used for Administrator module for SharePoint 2013 environments. After deploying it, go to SharePoint to active the features for each site collection: **DocAve Security Management Feature**, **DocAve Security Management Ribbon**, **DocAve Security Search History Feature** and **DocAve Security Search Result Feature**. For more information, refer to the Administrator User Guide.

  ***Note**: In order to use the **SP2013SecurityManagement** feature successfully, you must restart the timer service on your server with SharePoint 2013. Navigate to **Start** > **Administrative Tools** > **Services**, Select **SharePoint Timer Service**, and click **Restart the service**.

- **SP2013EndUserGranularRestore.wsp** – This solution is only used for the Granular Backup and Restore module for the SharePoint 2013 environment. After deploying it, navigate to **DocAve Manager** > **Data Protection** > **Granular Backup and Restore** > **Restore** > **End-User Restore**, and select the desired farm, Web application, or site collection where you want to activate this solution. Click **Activate** on the ribbon to activate the solution. You can also go to SharePoint to activate the **End-User Restore for SharePoint 2013** feature for each site collection.

  ***Note:** This solution does not support the 2010 mode sites of SharePoint 2013. For more information, refer to the Granular Backup and Restore User Guide.

- **SP2013LotusNotesLinkTracking.wsp** – This solution is used to enhance the DocLinks migration process for SharePoint 2013.

- **SP2013AuditorMonitor.wsp** – This solution is only used for Report Center module for SharePoint 2013 environments. After deploying it, go to **Report Center** > **Settings** > **Auditor Controller** to activate this feature by selecting the **Site Collection Deletion** or **Site Creation** checkboxes in the **Audit Action** field. For more information, refer to the Report Center User Guide.

- **SP2013DocumentAuditing.wsp** – This solution is only used for Report Center module for SharePoint 2013 environments. After deploying it, go to **Report Center**> **Settings** > **Manage Features** to activate this feature at the site collection level. You can also activate this feature directly in SharePoint. This allows you to audit all documents under the specified site collection as well as view the auditor history of documents in the site collection. For more information, refer to the Report Center User Guide.

- **SP2013UsageActivityWebParts.wsp** – This solution is only used for the Report Center module for SharePoint 2013 environments. After deploying it, you will be able to enable the **AvePoint Social Activity Web Parts** feature at site collection level, allowing you to add Social Activity Web Parts in SharePoint sites. These Web parts display the reports on social activities and contents within a specific farm/Web application/site collection/site. The six Web parts in SharePoint 2013 are Most Active Contributors, Most Popular Contributors, Top Documents, Top Blog Posts, Top Discussions, and Top Wiki Pages.

  ***Note:** The Most Popular Contributors Web Part does not support SharePoint 2010.

- **SP2013AlternateFileAccess.wsp** – This solution is used to upload the large files or the files with the file types that cannot be uploaded to SharePoint directly. It is only used for the Storage Manager module for SharePoint 2013 environments. After deploying it, navigate to **Storage Optimization** > **Real-Time Storage Manager** or **Scheduled Storage Manager** > **Manage Feature**, and select the desired farm, Web application, or site collection where you want to activate this solution. Click **Activate** to activate the solution. You can also go to SharePoint to activate the **Alternate File Access** site collection feature for each site collection. For more information, refer to Storage Manager User Guide.

- **SP2013ConnectorContentLibrary.wsp** – This solution is used for the Connector module and the Cloud Connect module in SharePoint 2013 environments. After deploying it, you enable the feature at the site collection level. For more information, refer to the Connector User Guide and the Cloud Connect User Guide.

- **SP2013ConnectorMediaLibrary.wsp** – This solution is used for the Connector module and the Cloud Connect module in SharePoint 2013 environments. After deploying it, you enable the feature at the site collection level. For more information, refer to the Connector User Guide and the Cloud Connect User Guide.

- **SP2013EndUserArchiver.wsp** – This solution is only used for the Archiver module for SharePoint 2013 environments. After deploying it, you are able to use End User Archiving in Archiver and end users are able to archive data by directly SharePoint 2013. For more information, refer to the Archiver User Guide.

- **SP2013ErrorPageforArchivedData.wsp** – This solution is only used for Archiver module for SharePoint 2013 environments. After deploying it, when an item has been archived and a user want to open the archived item using the original URL, DocAve will check if

the item has already been archived, if yes, the user will see a prompt message. For more information, refer to the Archiver User Guide.

- **SP2013PreviewGUI.wsp –** This solution is used to preview the files in SharePoint. It is only used for the SharePoint 2013 environments. After deploying it, you will be able to enable the corresponding feature at the site collection level, allowing you to preview the files in SharePoint 2013. For more information, refer to the Connector User Guide.
- **SP2013StorageManagerStubTraceManagement.wsp –** This solution is used to show the externalized details for the documents and attachments in SharePoint 2013. After the solution is deployed, navigate to **Storage Optimization** > **Real-Time Storage Manager** or **Scheduled Storage Manager** > **Manage Feature** > **Stub Trace**. Click **Activate All** to activate the **Stub Tracing** feature on all of the site collections in the selected Web application, or click **Activate** to activate the **Stub Tracing** feature on the selected site collection. For more information, refer to DocAve Storage Manager User Guide.

Storage Configuration

Storage Configuration allows you to create and configure physical and logical devices or storage policies for certain DocAve modules to store backup data.

Physical Device

Physical devices allow DocAve to store backup data. In order for DocAve to recognize a physical device for use, it must first be configured.

*__Note__: Depending on where you want to store the backup data, DocAve has the capability to write to any **Net Share**, **FTP**, **Amazon S3**, **AT&T Synaptic**, **Box**, **Caringo Storage**, **DELL DX Storage**, **Dropbox**, **EMC Atmos**, **EMC Centera**, **HDS Hitachi Content Platform**, **IBM Storwize Family**, **Microsoft Azure Storage**, **NFS**, **OneDrive**, **Rackspace Cloud File**, and **TSM** devices.

To access **Physical Device** settings for DocAve, go to the **Control Panel** interface and click **Physical Device** under the **Storage Configuration** heading. You will be brought to the **Storage Configuration** interface with the **Physical Device** tab selected. Click **Close** on the ribbon to close the **Storage Configuration** interface.

In the **Physical Device** configuration interface, you will see a list of physical devices under the **Physical Device** tab and two pie charts containing **Data Usage** information by the physical devices. The chart on the left displays the share of data stored on each physical device type. The chart on the right displays the amount of storage used for storing SharePoint BLOBs versus the amount of storage used for storing DocAve native data; you can configure the physical device type you want this chart to display by clicking on the drop-down menu above the chart, and then selecting from: **All Physical Devices**, **Net Share**, **FTP**,

Amazon S3, **AT&T Synaptic**, **Box**, **Dropbox**, **EMC Atmos**, **HDS Hitachi Content Platform**, **IBM Storwize Family**, **Microsoft Azure Storage**, **NFS**, **OneDrive**, **Rackspace Cloud File**, and **TSM**.

To update the storage space information in the **Space Usage** column of the list of physical devices, as well as the data usage information presented in the pie charts in the **Data Usage** section, click **Refresh** on the ribbon or the **Refresh** button under the **Physical Device** tab on the interface.

Managing Physical Devices

In **Storage Configuration**, you can create a new physical device, view details about a physical device, edit a previously configured physical device, or delete a previously configured physical device. For details on creating or editing a physical device, see the Configuring Physical Devices section of this guide.

To view details about a physical device, select it from the list of previously configured physical devices, and then click **View Details** on the ribbon. You will see all of the detailed information about the specific physical device displayed in the following three tabs:

- **Summary** – The configurations for this physical device.
- **Associated Logical Device** – The logical devices that use this physical device.
- **Data** – The size of the data stored in this physical device.

Click **Edit** on the ribbon to change the configurations for this physical device. For details on editing configurations for a physical device, see the Configuring Physical Devices section of this guide.

To delete a physical device from DocAve, select a physical device from the list of physical devices, and then click **Delete** on the ribbon. A confirmation window will pop- up and ask if you are sure you want to proceed with the deletion. Click **OK** to delete the selected physical devices, or click **Cancel** to return to the **Storage Configuration** interface without deleting the selected physical devices.

***Note:** The physical device cannot be deleted if it is currently being used by one or more plans/profiles.

Configuring Physical Devices

To create a new physical device, click **Create** on the ribbon, and then select **Physical Device** from the drop-down menu. To modify a previously configured physical device, select the physical device, and then click **Edit** on the ribbon. Because DocAve supports a number of types of physical devices, each device type requires different configurations. In the sections that follow, you will find instructions on configuring the following types of physical devices: **Net Share**, **FTP**, **Amazon S3**, **AT&T Synaptic**, **Box**, **Caringo Storage**, **DELL DX Storage**, **Dropbox**, **EMC Atmos**, **EMC Centera**, **HDS Hitachi Content Platform**, **IBM Storwize Family**, **Microsoft Azure Storage**, **NFS**, **OneDrive**, **Rackspace Cloud File**, and **TSM**.

***Note**: For physical devices with the **Advanced** option, refer to the information below.

- Only use the extended parameters to fulfill your special requirements.

- Except for the **FileSpace** parameter of TSM, all of the extended parameters and their values are not case-sensitive.

Net Share

In the **Create Physical Device** or **Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device. Then, enter an optional **Description** for future reference.
2. **Storage Type** – Select **Net Share** from the drop-down list.
3. **Storage Type Configuration** – Configure the following settings:
    - **UNC path** – Enter a path in the **UNC path** text box. If the path you entered does not exist, it will be created automatically.
    - **Specify a managed account profile** – Select a managed account profile from the drop-down list to access the entered UNC path.
    - **Advanced** – Enter the following extended parameters in advanced settings if necessary. If you have multiple parameters to enter, press **Enter** on the keyboard to separate the parameters. Refer to the instructions below to add parameters:
        - **IsRetry** – Whether or not to try again when DocAve failed to write the data in the physical device.
            - If you enter **IsRetry=true**, it will try again when DocAve failed to write the data in the physical device.
            - If you enter **IsRetry=false**, it will not try again when DocAve failed to write the data in the physical device.
        - **BufferSize** – Configure the size of the temporary storage of data. The format is **BufferSize =1**. The unit is **MB**.
        - **SecurelyDelete** – Overwrites the BLOB data stored in the Net Share physical devices seven times with empty strings before deleting it thoroughly for the security reasons.
            - If you enter **SecurelyDelete=true**, DocAve will enable this function and overwrite the BLOB data before deleting it.
            - If you enter **SecurelyDelete=false**, DocAve will not enable this function nor overwrite the BLOB data before deleting it.
        - **AuthMethod** – Enable different permission validation methods for different users to visit Net Share.
            - If you enter **AuthMethod=LogonUser**, it will enable LogonUser user permission validation method.
            - If you enter **AuthMethod=NetUse**, it will enable NetUse user permission validation method.

- If you enter **AuthMethod=NetUse_DeleteOld**, it will enable NetUse user permission validation method and delete the previous validation method.

Click **Validation Test**. DocAve will test the path and user information to make sure they are valid.

4. **Space Threshold** – Set up the space threshold for the physical device. Once the threshold is reached, data will stop being written to the physical device and the device will become read-only. There are two methods you can select:
    - **Less than … MB** – Enter the minimum size of the free space for the physical device, if the free space of the physical device is less than the entered size, data will stop being written to the physical device and the device will become read-only. By default, this option is used and the default size is 1024 MB. The size you enter into the text box must be equal to or larger than 1024MB.
    - **Less than … %** – Enter the minimum percentage of the free space, if the free space of the physical device is less than the entered percentage, data will stop being written to the physical device and the device will become read-only.

    Click **Test** to verify the space or percentage you entered.

Click **Save** to save the configurations and return to the **Storage Configuration** interface. After the physical device is saved, it will be listed in the **Physical Device** tab.

FTP

In the **Create Physical Device** or **Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device. Then, enter an optional **Description** for future reference.
2. **Storage Type** – Select **FTP** from the drop-down list.
3. **Storage Type Configuration** – Configure the following settings:
    - **Host** – Enter the IP address of the FTP server.
    - **Port** – Enter the port to use to connect to this FTP server. The default port is 21.
    - **Username** – Enter the username to use to connect to this FTP server.
    - **Password** – Enter the password of the specified username.
    - **Advanced** – Enter the following extended parameters in advanced settings if necessary. If you have multiple parameters to enter, press **Enter** on the keyboard to separate the parameters. Refer to the instructions below to add parameters:
        - **ftpType=win03** – Whether or not the ftp is the ftp in the Windows 2003 operating system.
        - **IsRetry** – Whether or not to try again when DocAve failed to write the data in the physical device.

        - If you enter **IsRetry=true**, it will try again when DocAve failed to write the data in the physical device.
        - If you enter **IsRetry=false**, it will not try again when DocAve failed to write the data in the physical device.
    - **RetryInterval**– Customize the retry interval when the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30 represents the interval between the network interruption and reconnection is 30 milliseconds.

      If you do not configure this parameter, the value is 30 seconds by default.
    - **RetryCount**– Customize the reconnection times after the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646. For example, RetryCount=60 represents when the network connection is interrupted, it can reconnect at most 60 times.

      If you do not configure this parameter, the value is 6 by default.

Click **Validation Test** to verify that the information you entered is correct.

Click **Save** to save the configurations and return to the **Storage Configuration** interface, or click **Cancel** to return to the **Storage Configuration** interface without saving any changes. After the physical device is saved, it will be listed in the Physical Device tab.

Amazon S3

In the **Create Physical Device** or **Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device, and enter an optional **Description** for future reference.
2. **Storage Type** – Select **Amazon S3** from the drop-down list.
3. **Storage Type Configuration** – Configure the following settings:
    - **Bucket name** – Enter the bucket name you wish to access.
    - **Access key ID –** Enter the corresponding access key ID to access the specified bucket. You can view the **Access key ID** from your AWS account.
    - **Secret access key** – Enter the corresponding secret key ID to access the specified bucket. You can view the **Secret access key** from your AWS account.
    - **Storage region** – Select the **Storage region** of this bucket from the drop-down menu. The available regions are US Standard, US West (Northern California), EU (Ireland), Asia Pacific (Singapore), and Asia Pacific (Tokyo).
    - **Advanced** – Enter the following extended parameters in **Advanced** settings if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.

- **RetryInterval** – Customize the retry interval when the network connection is interrupted. Enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30000 represents the interval between the network interruption and reconnection is 30000 milliseconds.

  If you do not configure this parameter, the value is 30 seconds by default.

- **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer between 0 and 2147483646. For example, RetryCount=6 represents when the network connection is interrupted, it can reconnect at most 6 times.

  If you do not configure this parameter, the value is 6 by default.

- **CustomizedMetadata** – Configure if DocAve customized metadata or user-added metadata is supported. By default, DocAve customized metadata and user added metadata are all supported in DocAve.
- **CustomizedMode=Close –** This physical device will not support DocAve customized metadata or user added metadata.
- **CustomizedMode=SupportAll** – This physical device will support all DocAve customized metadata and user added metadata.
- **CustomizedMode=DocAveOnly** – This physical device will only support DocAve customized metadata.
- **CustomizedMode=CustomizedOnly** – This physical device will only support user-added metadata.

Click **Validation Test** to verify that the information you entered is correct.

Click **Save** to save the configurations and return to the **Storage Configuration** interface, or click **Cancel** to return to the **Storage Configuration** interface without saving any changes. After the physical device is saved, it will be listed in the **Physical Device** tab.

AT&T Synaptic

In the **Create Physical Device** or **Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device. Then enter an optional **Description** for future reference.
2. **Storage Type** – Select **AT&T Synaptic** from the drop-down list.
3. **Storage Type Configuration** – Configure the following settings:
   - **Root folder** – Enter the **Root folder** where you wish to access.
   - **Full token ID –** Enter the corresponding **Full token ID** (commonly referred to as the UID) to access the specified root folder.
   - **Shared secret** – Enter the corresponding **Shared secret** (commonly referred to as the UID) to access the specified root folder.

- **Advanced** – Enter the following extended parameters in **Advanced** settings if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.
    - **RetryInterval** – Customize the retry interval when the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30000 represents the interval between the network interruption and reconnection is 30000 milliseconds.

      If you do not configure this parameter, the value is 30 seconds by default.
    - **RetryCount** – Customize the reconnection times after the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646. For example, RetryCount=6 represents when the network connection is interrupted, it can reconnect at most 6 times.

      If you do not configure this parameter, the value is 6 by default.
    - **CustomizedMetadata** – Configure if DocAve customized metadata or user-added metadata is supported. By default, DocAve customized metadata and user-added metadata are all supported in DocAve.
    - **CustomizedMode=Close –** This physical device will not support DocAve customized metadata or user-added metadata.
    - **CustomizedMode=SupportAll** – This physical device will support all DocAve customized metadata and user-added metadata.
    - **CustomizedMode=DocAveOnly** – This physical device will only support DocAve customized metadata.
    - **CustomizedMode=CustomizedOnly** – This physical device will only support user-added metadata.

  Click **Validation Test** to verify that the information you entered is correct.

Click **Save** to save the configurations and return to the Storage Configuration interface, or click **Cancel** to return to the Storage Configuration interface without saving any changes. After the physical device is saved, it will be listed in the **Physical Device** tab.

Box

In the **Create Physical Device** or **Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device. Then, enter an optional **Description** for future reference.
2. **Storage Type** – Select **Box** from the drop-down list.
3. **Storage Type Configuration** – Configure the following settings:
    - **Root Folder Name** – Enter the folder name you want to synchronize with this library.

- **E-mail address** – Enter the e-mail address to access Box.
- **Token storage location** – Enter the UNC path of the location where the token's file resides.

  ***Note:** By clicking the link in the **Retrieve Token** step or the link on the **Token** page of **StorageTokenClient** tool, select a directory to store the downloaded token's file. For details about how to run the **StorageTokenClient** tool, refer to DocAve 6 Supplementary Tools User Guide.*
- **Username** – Enter the username to access the token storage location.
- **Password** – Enter the relevant password for the user.
- **Enable As-User** – Enter the e-mail address of the user whose Box data you want to view and manage.
  - **As-User e-mail address** – Enter the e-mail address of the user whose Box data you want to review and manage. Enter the e-mail address in the format: someone@exapmple.com.
- **Use the client information provided by DocAve** – Grant certain permissions to the application provided by DocAve so that you can access and manage the data of the entered account through DocAve.
  - **Retrieve Token** – Click **Retrieve Token**, enter the e-mail address and the password of Box in the pop-up window to log into Box and then a link will appear in this pop-up window. Click this link and download the token's file to a specific directory.

    ***Note:** Enter the administrator's e-mail address and the password of Box if the **Enable As-User** checkbox is selected.*
- **Use my client information** – Grant certain permissions to the application provided by yourself so that you can access and manage the data of certain account through DocAve. The account information is specified when you use the **StorageTokenClient** tool to generate tokens.

  ***Note:** The **StorageTokenClient** tool resides in the …\DocAve6\Manager\Shared\Tools\StorageTool\StorageTokenTool directory.*
- **Advanced** – Enter the following extended parameters in the advanced settings if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.
  - **RetryInterval** – Customize the retry interval when the network connection is interrupted. The default value is 30000 milliseconds. You are allowed to enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30 represents the interval between the network interruption and reconnection is 30 milliseconds.

    If you do not configure this parameter, the value is 30 seconds by default.

- **RetryCount** – Customize the reconnection times after the network connection is interrupted. The default value is 6. You are allowed to enter any positive integer between 0 and 2147483646. For example, RetryCount=10 represents when the network connection is interrupted, it can reconnect at most 10 times.

  If you do not configure this parameter, the value is 6 by default.

Click **Validation Test** to verify that the information you entered is correct.

4. **Space Threshold** – Set up the space threshold for the physical device. Once the threshold is reached, data will stop being written to the physical device and the device will become read-only. There are two methods you can select:

   - **Less than … MB** – Enter the minimum size of the free space for the physical device, if the free space of the physical device is less than the entered size, data will stop being written to the physical device and the device will become read-only. By default, this option is used and the default size is 1024 MB. The size you enter into the text box must be equal to or larger than 1024MB.
   - **Less than … %** – Enter the minimum percentage of the free space, if the free space of the physical device is less than the entered percentage, data will stop being written to the physical device and the device will become read-only.

   Click **Test** to verify the space or percentage you entered.

Click **Save** to save the configurations and return to the **Storage Configuration** interface, or click **Cancel** to return to the **Storage Configuration** interface without saving any changes. After the physical device is saved, it will be listed in the **Physical Device** tab.

***Note:** End-users will configure a Cloud Connect storage path on the library level to directly connect existing file share content to a SharePoint library. DocAve Cloud Connect only supports **Box** storage on the library level. To configure a Cloud Connect path on the library level in DocAve, **Box** is selected as the storage type by default. For more information, refer to the Cloud Connect User Guide.

Caringo Storage

In the **Create Physical Device** or **Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device. Then, enter an optional **Description** for future references.
2. **Storage Type** – Select **Caringo Storage** from the drop-down list.
3. **Storage Type Configuration** – Configure the following settings:

   - **Communication type** – There are two available ways to communicate with server.
     - **Proxy Locator** – In this type, enter CNS private network IP and Cluster name, DocAve can find information of storage node. The DocAve server and the Caringo server must be in the same subnet. Refer to Configuring Proxy Locator for more information.

- **Static Locator** – In this type, enter the storage node IP address. DocAve will visit the storage node you configured directly. If you have multiple storage nodes, enter their IP addresses and use semicolons to separate the entered IP addresses. Refer to Configuring Static Locator for more information.

- **Require authentication** – Enable user authentication when visiting the server. Enter username and password for authentication. **Authentication realm** is the realm that the user you specified belongs to.
- **With remote D/R cluster** – Check this checkbox if you wish to use the remote cluster when the local cluster is not available. Select an **Access mode** from the drop-down menu, and then configure the following settings:
  - **Remote CSN** – If this mode is selected, enter the **Remote CSN host** (the hostname or IP address of the Remote cluster storage node) and **Remote CSN port** (the port used to access the Cluster) used to access the cluster. The default port is 80.
  - **Local Proxy** – If this mode is selected, enter the **SCSP proxy host** (the hostname or IP address of the SCSP Proxy host configured by the customer), **SCSP proxy port** (the port used to access the SCSP Proxy host, 80 is the default port) and the **Remote cluster name** used to access the cluster.
- **Number of object replicas** – Enter the number of replicas of the data.
- **Caringo optimizer compression** – Select a compression method for the data stored in the Caringo Storage:
  - **None** – The data will not be compressed. This is selected by default.
  - **Fast** – The compression time is shorter, and the compression rate is lower. This means that the size of the data will not be reduced by as much as if **Best** is selected, but the process will not take as long.
  - **Best** – The compression time is longer, and the compression rate is higher. This means that the size of the data will be reduced much more than if **Fast** is selected, but the process will take more time.
- **Compress after (Days)** – Enter a positive integer between 0 and 29 for the number of days you wish to delay data compression after it is stored.
- **Advanced** – Enter the following extended parameters in advanced settings if necessary. If you have multiple parameters to enter, press **Enter** on the keyboard to separate the parameters. Refer to the instructions below to add parameters.
  - **LocatorType** – Add a customized Locator type, the default type is Proxy. Refer to Configuring Locator Type for more information.
  - **CustomizedMetadata** – Allow you to write customized metadata into the data.

The metadata format must be, for example: CustomizedMetadata={[testkey1,testvalue1],[testkey2,testvalue2],[testkey3,testvalue3]……}

You are allowed to customize testkey and testvalue group number. Use "," to separate the testkeys and testvalues.

- **CustomizedMode** – Allow you to configure if DocAve customized metadata or user-added metadata is supported. By default, DocAve customized metadata and user-added metadata are all supported in DocAve. Note that before entering this parameter, you have to configure **With remote D/R cluster** and enter the corresponding configuration data. Refer to Configuring Customized Mode for more information.
- **CacheRemoteHost** – Allow you to cache the information of the RemoteHost. Refer to the Configuring Cache Remote Host section for more information.
- **RemoteHostTimeout** – Allow you to customize the time to cache the RemoteHost information before the information is deleted. You are allowed to enter any positive integer between 0 and 2147483646 (the unit is second). For example, if you enter **RemoteHostTimeout=36000**, it represents that the cache time is 36000 seconds.

Click **Validation Test** to verify that the information you entered is correct.

Click **Save** to save the configurations and return to the **Storage Configuration** interface, or click **Cancel** to return to the **Storage Configuration** interface without saving any changes. After the physical device is saved, it will be listed in the **Physical Device** tab.

Configuring Proxy Locator

To configure the proxy locator, complete the following steps:

1. **CSN private network IP** – Enter the hostname or IP address of the node.
2. **SCSP proxy port** – Enter the port to use to connect to the cluster. The default port is 80.
3. **Cluster name** – Enter the name of the cluster you wish to access.

Configuring Static Locator

To configure the static locator, complete the following steps:

1. **Primary DX storage node** – Enter the hostname or IP address of the node, if you are entering multiple nodes, separate each node using ;
2. **Primary DX Storage node port** – Enter the port used to connect to the primary DX storage node. The default port is 80.
3. **Primary DX CR publisher** – You can keep it empty for now.
4. **Primary DX CR publisher port** – You can keep it empty for now.

Configuring Locator Type

To configure the locator type, complete the following steps:

- If you enter **LocatorType=Proxy**, it represents you will use Proxy locator.
- If you enter **LocatorType=Static**, it represents you will use Static locator.

Configuring Customized Mode

To configure the customized mode, complete the following steps:

- If you enter **CustomizedMode=Close**, it represents this physical device will not support DocAve customized metadata or user-added metadata.
- If you enter **CustomizedMode=SupportAll**, it represents this physical device will support all DocAve customized metadata and user-added metadata.
- If you enter **CustomizedMode=DocAveOnly**, it represents this physical device will only support DocAve customized metadata.
- If you enter **CustomizedMode=CustomizedOnly**, it represents this physical device will only support user-added metadata.

Configuring Cache Remote Host

To configure the cache remote host, complete the following steps:

- If you enter **CacheRemoteHost=true**, it represents this physical device will cache the RemoteHost information.
- If you enter **CacheRemoteHost=false**, it represents this physical device will not cache the RemoteHost information.

Dell DX Storage

In the **Create Physical Device** or **Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device. Then, enter an optional **Description** for future reference.
2. **Storage Type** – Select **Dell DX Storage** from the drop-down list.
3. **Storage Type Configuration** – Configure the following settings:
    - **CSN private network IP** – Enter the hostname or IP address of the node.
    - **SCSP proxy port** – Enter the port to use to connect to the cluster. The default port is 80.
    - **Cluster name** – Enter the name of the cluster you wish to access.
    - **Primary DX CR publisher** – You can keep it empty for now.
    - **Primary DX CR publisher port** – You can keep it empty for now.

- **With remote D/R cluster** – Check this checkbox if you wish to use the remote cluster when the local cluster is not available. Select an **Access mode** from the drop-down menu, and then configure the following settings:
    - **Remote CSN** – If this mode is selected, enter the **Remote CSN host** (the hostname or IP address of the Remote cluster storage node) and **Remote CSN port** (the port used to access the Cluster) used to access the cluster. The default port is 80.
    - **Local Proxy** – If this mode is selected, enter the **SCSP proxy host** (the hostname or IP address of the SCSP Proxy host configured by the customer), **SCSP proxy port** (the port used to access the SCSP Proxy host, 80 is the default port) and the **Remote cluster name** used to access the cluster.
- **Number of object replicas** – Enter the number of replicas of the data.
- **DX optimizer compression** – Select a compression method for the data stored in the Dell DX Storage:
    - **None** – The data will not be compressed. This is selected by default.
    - **Fast** – The compression time is shorter, and the compression rate is lower. This means that the size of the data will not be reduced by as much as if **Best** is selected, but the process will not take as long.
    - **Best** – The compression time is longer, and the compression rate is higher. This means that the size of the data will be reduced much more than if **Fast** is selected, but the process will take more time.
- **Compress after (Days)** – Enter a positive integer between 0 and 29 for the number of days you wish to delay data compression after it is stored.
- **Advanced** – Enter the following extended parameters in advanced settings if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.
    - **LocatorType** – Add a customized locator type. The default type is Proxy. If you enter **LocatorType=Proxy**, it represents you will use Proxy locator. If you enter **LocatorType=Static**, it represents you will use Static locator.
    - **CustomizedMetadata** – Allows you to write customized metadata into the data. The metadata format must be, for example: CustomizedMetadata={[testkey1,testvalue1],[testkey2,testvalue2],[testkey3,testvalue3]……}. You are allowed to customize testkey and testvalue group number. Use "," to separate the entered testkeys and testvalues.
    - **CustomizedMode** – Allows you to configure if DocAve customized metadata or user-added metadata is supported. By default, DocAve customized metadata and user-added metadata are all supported in DocAve. Note that before entering this parameter, you have to configure **With remote D/R cluster** and enter the corresponding configuration data. Refer to the Configuring Customized Mode section for more information.

Click **Validation Test** to verify that the information you entered is correct.

4. **Space Threshold** – Set up the **Space Threshold** for the physical device. Once the threshold is reached, data will stop being written to the physical device and the device will become read-only. There are two methods you can select:
    - **Less than … MB** – Enter the minimum size of the free space for the physical device, if the free space of the physical device is less than the entered size, data will stop being written to the physical device and the device will become read-only. By default, this option is used and the default size is 1024MB.
    - **Less than … %** – Enter the minimum percentage of the free space, if the free space of the physical device is less than the entered percentage, data will stop being written to the physical device and the device will become read-only.

    Click **Test** to verify the space or percentage you entered.

Click **Save** to save the configurations and return to the Storage Configuration interface, or click **Cancel** to return to the **Storage Configuration** interface without saving any changes. After the physical device is saved, it will be listed in the **Physical Device** tab.

Configuring Customized Mode

To configure customized mode, complete the following steps:

- If you enter **CustomizedMode=Close**, this physical device will not support DocAve customized metadata or user-added metadata.
- If you enter **CustomizedMode=SupportAll**, this physical device will support all DocAve customized metadata and user-added metadata.
- If you enter **CustomizedMode=DocAveOnly**, this physical device will only support DocAve customized metadata.
- If you enter **CustomizedMode=CustomizedOnly**, this physical device will only support user-added metadata.

Dropbox

In the **Create Physical Device** or **Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device. Then enter an optional **Description** for future reference.
2. **Storage Type** – Select **Dropbox** from the drop-down list.
3. **Storage Type Configuration** – Configure the following settings:
    - **Root folder –** Enter a name for the root folder which will be created in the DropBox and used to store the data.

- **Access token** – Enter the token appeared in the **Retrieve Token** step, or the token which is obtained by the **StorageTokenClient** tool in this text box.
- **Use the client information provided by DocAve –** Grant certain permissions to the application provided by DocAve so that you can access and manage the data of the entered account through DocAve.
    - **Retrieve Token** – Click **Retrieve Token**, enter the e-mail address and the password of Dropbox in the pop-up window to log into Dropbox, and then the token will appear in this pop-up window.
- **Use my client information** – Grant certain permissions to the application provided by yourself so that you can access and manage the data of certain account through DocAve. The account information is specified when you use the **StorageTokenClient** tool to generate tokens.

  ***Note:** The **StorageTokenClient** tool resides in the …\DocAve6\Manager\Shared\Tools\StorageTool\StorageTokenTool directory.
- **Advanced –** Enter the following extended parameters in advanced settings if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.
    - **RetryInterval** – Customize the retry interval when the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30 represents the interval between the network interruption and reconnection is 30 milliseconds.

      If you do not configure this parameter, the value is 30 seconds by default.
    - **RetryCount** – Customize the reconnection times after the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646. For example, RetryCount=10 represents when the network connection is interrupted, it can reconnect at most 10 times.

      If you do not configure this parameter, the value is 6 by default.

Click **Validation Test** to verify that the information you entered is correct.

4. **Space Threshold** – Set up the **Space Threshold** for the physical device. Once the threshold is reached, data will stop being written to the physical device and the device will become read-only. There are two methods you can select:
    - **Less than … MB** – Enter the minimum size of the free space for the physical device. If the free space of the physical device is less than the entered size, data will stop being written to the physical device and the device will become read-only. By default, this option is used and the default size is 1024MB.
    - **Less than … %** – Enter the minimum percentage of the free space. If the free space of the physical device is less than the entered percentage, data will stop being written to the physical device and the device will become read-only.

Click **Test** to verify the space or percentage you entered.

Click **Save** to save the configurations and return to the Storage Configuration interface, or click **Cancel** to return to the Storage Configuration interface without saving any changes. After the physical device is saved, it will be listed in the **Physical Device** tab.

EMC Atmos

In the **Create Physical Device** or **Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device. Then enter an optional **Description** for future reference.
2. **Storage Type** – Select **EMC Atmos** from the drop-down list.
3. **Storage Type Configuration** – Configure the following settings:
    - **Interface Type** – Select **Namespace** or **Object** from the drop-down list.
        - **Namespace** – Namespace Interface EMC Atmos physical device can be used by all of the DocAve modules that leverage physical devices.
        - **Object** – Object Interface EMC Atmos physical device can only be used by Storage Manager.
    - **Access point** – Enter the URL which will be used to connect to Atmos Online. The default URL is *http://accesspoint.emccis.com*.
    - **Root folder** – Enter the **Root folder** where you wish to access. If you select **Object** as the **Interface Type**, the **Root folder** will be hidden and not displayed on GUI.
    - **Full token ID –** Enter the corresponding **Full token ID** (commonly referred to as the UID) to access the specified root folder.
    - **Shared secret** – Enter the corresponding **Shared secret** (commonly referred to as the UID) to access the specified root folder.
    - **Advanced** – Enter the following extended parameters in **Advanced** settings if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.
        - **RetryInterval** – Customize the retry interval when the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30 represents the interval between the network interruption and reconnection is 30 milliseconds.

          If you do not configure this parameter, the value is 30 seconds by default.

        - **RetryCount** – Customize the reconnection times after the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646. For example, RetryCount=10 represents when the network connection is interrupted, it can reconnect at most 10 times.

If you do not configure this parameter, the value is 6 by default.

- **CustomizedMetadata** – Configure if DocAve customized metadata or user-added metadata is supported. By default, DocAve customized metadata and user-added metadata are all supported in DocAve.
- **CustomizedMode=Close –** This physical device will not support DocAve customized metadata or user-added metadata.
- **CustomizedMode=SupportAll** – This physical device will support all DocAve customized metadata and user-added metadata.
- **CustomizedMode=DocAveOnly** – This physical device will only support DocAve customized metadata.
- **CustomizedMode=CustomizedOnly** – This physical device will only support user-added metadata.
- **EnableChecksumForCreate** – Configure whether to enable the function to check data integrity when writing data. The default value for EnableChecksumForCreate is false.
- **VerifyChecksumAtRead** –Configure whether to enable the function to check data integrity when reading data. The default value for VerifyChecksumAtRead is false.

Click **Validation Test** to verify that the information you entered is correct.

Click **Save** to save the configurations and return to the Storage Configuration interface, or click **Cancel** to return to the **Storage Configuration** interface without saving any changes. After the physical device is saved, it will be listed in the **Physical Device** tab.

EMC Centera

In the **Create Physical Device** or **Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device. Then, enter an optional **Description** for future reference.
2. **Storage Type** – Select **EMC Centera** from the drop-down list.
3. **Storage Type Configuration** – Configure the following settings:
   - **Centera cluster address** – Enter the IP address of the EMC Centera cluster.
   - **Authentication** – Select one authentication methods to connect to the EMC Centera cluster, refer to the Authentication Configuration section for more information.

   Click **Validation Test** to verify that the information you entered is correct.
4. **Space Threshold** – Set up the space threshold for the physical device. Once the threshold is reached, data will stop being written to the physical device and the device will become read-only. There are two methods you can select:

- **Less than … MB** – Enter the minimum size of the free space for the physical device, if the free space of the physical device is less than the entered size, data will stop being written to the physical device and the device will become read-only. By default, this option is used and the default size is 1024 MB.
- **Less than … %** – Enter the minimum percentage of the free space, if the free space of the physical device is less than the entered percentage, data will stop being written to the physical device and the device will become read-only.

Click **Test** to verify the space or percentage you entered.

Click **Save** to save the configurations and return to the Storage Configuration interface, or click **Cancel** to return to the **Storage Configuration** interface without saving any changes. After the physical device is saved, it will be listed in the **Physical Device** tab.

Authentication Configuration

To configure the Authentication, complete the following steps. Select one authentication methods to connect to the EMC Centera cluster:

- **Name/Secret Authentication** – If this option is chosen, you must then configure the following settings:
  - **Name** – Enter the name to connect to the EMC Centera cluster with.
  - **Secret** – Enter the secret for this name.
- **PEA files authentication** – If this option is chosen, you must then configure the following settings:
  - **PEA file location** – The location of the PEA file used to connect to the EMC Centera cluster.
  - **Location username** – Enter the username to use to access the PEA file location.
  - **Location password** – Enter the password of the specified Username used to access the PEA file location.

Click **Validation Test** to verify that the information you entered is correct.

HDS Hitachi Content Platform

In the **Create Physical Device** or **Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device. Then enter an optional **Description** for future references.
2. **Storage Type** – Select **HDS Hitachi Content Platform** from the drop-down list**.**
3. **Storage Type Configuration** – Configure the following settings:
   - **Primary namespace address** – Enter the primary Namespace Address where you want to store data.

For example, you can enter *http://ns0.ten1.hcp.storage1.com.* Make sure the URL entered here can be accessed by the DocAve Control service, Media service and the corresponding DocAve Agent(s).

- **Secondary namespace address** (Optional) – Enter the secondary Namespace Address which will be used to store data when the primary Namespace Address is not accessible. This namespace address is used in conjunction with the **FailOverMode** parameter. For the detailed information, refer to the Configuring FailOverMode section.

  ***Note**: The secondary Namespace must be mirrored to the primary Namespace.

  For example, you can enter *http://ns0.ten1.hcp.storage2.com.* Make sure the URL entered here can be accessed by the DocAve Control service, Media service and the corresponding DocAve Agent(s).

- **Root folder** – Enter the directory where you want to store data. The directory will be created automatically in the specified namespace address if it does not exist. For example, *directoryName*.
- **Username and Password** – The user name and password to access the namespace you entered.
- **Advanced** –Enter the following extended parameters in advanced settings if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.
  - **RetryInterval** – Enter the time interval of the **Retry** operation when the connection with the HDS Hitachi Content Platform server is not available. The format is **RetryInterval=200**. The unit for this parameter is **millisecond**.

    If you do not configure this parameter, the value is 30 seconds by default.
  - **RetryCount** – Enter the count of the **Retry** operation when the connection with the HDS Hitachi Content Platform server is not available. The format is **RetryCount=6**.

    If you do not configure this parameter, the value is 6 by default.
  - **FlushDNS** – Enter whether to flush the DNS before connecting to the specified secondary Namespace Address. The format is **FlushDNS=true**.

    If you do not configure this parameter, the value is true by default, which means the DNS will be flushed before connecting to the specified secondary Namespace Address.
  - **FailoverMode** – Enter when to use the configured secondary Namespace Address if the primary Namespace Address is not accessible. Refer to Configuring FailoverMode for more information.

Click **Validation Test** to verify that the information you entered is correct.

4. **Space Threshold** – Set up the **Space Threshold** for the physical device. Once the threshold is reached, data will stop being written to the physical device and the device will become read-only. There are two methods you can select:

    - **Less than … MB** – Enter the minimum size of the free space for the physical device, if the free space of the physical device is less than the entered size, data will stop being written to the physical device and the device will become read-only. By default, this option is used and the default size is 1024 MB.
    - **Less than … %** – Enter the minimum percentage of the free space, if the free space of the physical device is less than the entered percentage, data will stop being written to the physical device and the device will become read-only.

    Click **Test** to verify the space or percentage you entered.

Click **Save** to save the configurations and return to the **Storage Configuration** interface, or click **Cancel** to return to the Storage Configuration interface without saving any changes. After the physical device is saved, it will be listed in the **Physical Device** tab.

Configuring FailoverMode

To configure FailoverMode, complete the following steps:

- If you enter **FailoverMode= ReadWrite**, the secondary Namespace Address will enable the upload and download function.
- If you enter **FailoverMode=Read**, the secondary Namespace Address will only enable the download function.
- If you enter **FailoverMode=Off**, the secondary Namespace Address will not be used.

IBM Storwize Family

In the **Create Physical Device** or **Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device. Then, enter an optional **Description** for future reference.
2. **Storage Type** – Select **IBM Storwize Family** from the drop-down list.
3. **Storage Type Configuration** – Configure the following settings:

    - **UNC path** – Enter a path in the **UNC path** text box. If the path you entered does not exist, it will be created automatically.
    - **Specify a managed account profile** – Select a managed account profile from the drop-down list to access the entered UNC path.
    - **Advanced** – Enter the following extended parameters in advanced settings if necessary. If you have multiple parameters to enter, press **Enter** on the keyboard to separate the parameters. Refer to the instructions below to add parameters:
        - **IsRetry** – Whether or not to try again when DocAve failed to write the data in the physical device.

        - If you enter **IsRetry=true**, it will try again when DocAve failed to write the data in the physical device.
        - If you enter **IsRetry=false**, it will not try again when DocAve failed to write the data in the physical device.
    - **BufferSize** – Configure the size of the temporary storage of data. The format is **BufferSize =1**. The unit is **MB**.
    - **SecurelyDelete** – Overwrites the BLOB data stored in the IBM Storwize Family physical devices seven times with empty strings before deleting it thoroughly for the security reasons.
        - If you enter **SecurelyDelete=true**, DocAve will enable this function and overwrite the BLOB data before deleting it.
        - If you enter **SecurelyDelete=false**, DocAve will not enable this function nor overwrite the BLOB data before deleting it.
    - **AuthMethod** – Enable different permission validation methods for different users to visit IBM Storwize Family.
        - If you enter **AuthMethod=LogonUser**, it will enable LogonUser user permission validation method.
        - If you enter **AuthMethod=NetUse**, it will enable NetUse user permission validation method.
        - If you enter **AuthMethod=NetUse_DeleteOld**, it will enable NetUse user permission validation method and delete the previous validation method.

    Click **Validation Test**. DocAve will test the path and user information to make sure they are valid.

4. **Space Threshold** – Set up the space threshold for the physical device. Once the threshold is reached, data will stop being written to the physical device and the device will become read-only. There are two methods you can select:
    - **Less than … MB** – Enter the minimum size of the free space for the physical device, if the free space of the physical device is less than the entered size, data will stop being written to the physical device and the device will become read-only. By default, this option is used and the default size is 1024 MB. The size you enter into the text box must be equal to or larger than 1024MB.
    - **Less than … %** – Enter the minimum percentage of the free space, if the free space of the physical device is less than the entered percentage, data will stop being written to the physical device and the device will become read-only.

    Click **Test** to verify the space or percentage you entered.

Click **Save** to save the configurations and return to the **Storage Configuration** interface, or click **Cancel** to return to the **Storage Configuration** interface without saving any changes. After the physical device is saved, it will be listed in the **Physical Device** tab.

Rackspace Cloud File

In the **Create Physical Device or Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device. Then, enter an optional **Description** for future reference.
2. **Storage Type** – Select **Rackspace Cloud File** from the drop-down list.
3. **Storage Type Configuration** – Configure the following settings:
    - **Container name** – Enter the **Container Name** you wish to access.
    - **Username –** Enter the corresponding **Username** to access the specified container.
    - **API key** – Enter the corresponding **API key** to access the specified container.
    - **CDN enabled** – Select this checkbox if the content delivery network (CDN) is enabled.
    - **Advanced** – Enter the following extended parameters in **Advanced** settings if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.
        - **RetryInterval** – Customize the retry interval when the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30 represents the interval between the network interruption and reconnection is 30 milliseconds.

          If you do not configure this parameter, the value is 30 seconds by default.
        - **RetryCount** – Customize the reconnection times after the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646. For example, RetryCount=10 represents when the network connection is interrupted, it can reconnect at most 10 times.

          If you do not configure this parameter, the value is 6 by default.
        - **CustomizedMetadata –** Configure if DocAve customized metadata or user-added metadata is supported. By default, DocAve customized metadata and user-added metadata are all supported in DocAve.
        - **CustomizedMode=Close –** This physical device will not support DocAve customized metadata or user-added metadata.
        - **CustomizedMode=SupportAll** – This physical device will support all DocAve customized metadata and user-added metadata.
        - **CustomizedMode=DocAveOnly** – This physical device will only support DocAve customized metadata.
        - **CustomizedMode=CustomizedOnly** – This physical device will only support user-added metadata.

Click **Validation Test** to verify that the information you entered is correct.

Click **Save** to save the configurations and return to the Storage Configuration interface, or click **Cancel** to return to the **Storage Configuration** interface without saving any changes. After the physical device is saved, it will be listed in the **Physical Device** tab.

NFS

In the **Create Physical Device** or **Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device. Then, enter an optional **Description** for future reference.
2. **Storage Type** – Select **NFS** from the drop-down list.
3. **Storage Type Configuration** – Configure the following settings:
    - **UNC path** – Enter a path in the **UNC path** text box. If the path you entered does not exist, it will be created automatically.
    - **Specify a managed account profile** – Select a managed account profile from the drop-down list to access the entered UNC path.
    - **Advanced** – Enter the following extended parameters in advanced settings if necessary. If you have multiple parameters to enter, press **Enter** on the keyboard to separate the parameters. Refer to the instructions below to add parameters:
        - **IsRetry** – Whether or not to try again when DocAve failed to write the data in the physical device.
            - If you enter **IsRetry=true**, it will try again when DocAve failed to write the data in the physical device.
            - If you enter **IsRetry=false**, it will not try again when DocAve failed to write the data in the physical device.
        - **BufferSize** – Configure the size of the temporary storage of data. The format is **BufferSize =1**. The unit is **MB**.
        - **SecurelyDelete** – Overwrites the BLOB data stored in the NFS physical devices seven times with empty strings before deleting it thoroughly for the security reasons.
            - If you enter **SecurelyDelete=true**, DocAve will enable this function and overwrite the BLOB data before deleting it.
            - If you enter **SecurelyDelete=false**, DocAve will not enable this function nor overwrite the BLOB data before deleting it.
        - **AuthMethod** – Enable different permission validation methods for different users to visit NFS.
            - If you enter **AuthMethod=LogonUser**, it will enable LogonUser user permission validation method.
            - If you enter **AuthMethod=NetUse**, it will enable NetUse user permission validation method.

- If you enter **AuthMethod=NetUse_DeleteOld**, it will enable NetUse user permission validation method and delete the previous validation method.

Click **Validation Test**. DocAve will test the path and user information to make sure they are valid.

Click **Save** to save the configurations and return to the **Storage Configuration** interface, or click **Cancel** to return to the **Storage Configuration** interface without saving any changes. After the physical device is saved, it will be listed in the **Physical Device** tab.

***Note**: Currently NFS is only supported by High Availability and Connector. For High Availability, to pass the validation test, Client for NFS feature must be installed on the Control server and user mapping is configured based on customer requirements. For Connector, to pass the validation test, Client for NFS feature must be installed on the Agent server.

OneDrive

In the **Create Physical Device** or **Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device. Then enter an optional **Description** for future reference.
2. **Storage Type** – Select **OneDrive** from the drop-down list.
3. **Storage Type Configuration** – Configure the following settings:
    - **Root Folder Name –** Enter a name for the root folder which will be created in the OneDrive and used to store the data.
    - **Refresh Token –** Enter the token from the **Retrieve Token** step, or the token which is obtained by the **StorageTokenClient** tool in this text box.
    - **Use the client information provided by DocAve** – Grant certain permissions to the application provided by DocAve so that you can access and manage the data of the entered account through DocAve.
        - **Retrieve Token** – Click **Retrieve Token**, enter the e-mail address and the password of OneDrive in the popup window to log into OneDrive, and then the token will appear in this pop-up window.
    - **Use my client information** – Grant certain permissions to the application provided by yourself so that you can access and manage the data of certain account through DocAve. The account information is specified when you use the **StorageTokenClient** tool to generate tokens.
        - **Client ID** – Enter the **Client ID** which is shown on the application page.
        - **Client Secret** – Enter the **Client Secret** which is shown on the application page.
        - **Redirect URL** – Enter the **Redirect URL** which is shown on the application page.

***Note:** The **StorageTokenClient** tool resides in the …\DocAve6\Manager\Shared\Tools\StorageTool\StorageTokenTool directory.

- **Advanced** – Enter the following extended parameters in advanced settings if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.
    - **RetryInterval** – Customize the retry interval when the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30 represents the interval between the network interruption and reconnection is 30 milliseconds.

      If you do not configure this parameter, the value is 30 seconds by default.
    - **RetryCount** – Customize the reconnection times after the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646. For example, RetryCount=10 represents when the network connection is interrupted, it can reconnect at most 10 times.

      If you do not configure this parameter, the value is 6 by default.

Click **Validation Test** to verify that the information you entered is correct.

4. **Space Threshold** – Set up the **Space Threshold** for the physical device. Once the threshold is reached, data will stop being written to the physical device and the device will become read-only. There are two methods you can select:
    - **Less than … MB** – Enter the minimum size of the free space for the physical device, if the free space of the physical device is less than the entered size, data will stop being written to the physical device and the device will become read-only. By default, this option is used and the default size is 1024MB.
    - **Less than … %** – Enter the minimum percentage of the free space, if the free space of the physical device is less than the entered percentage, data will stop being written to the physical device and the device will become read-only.

    Click **Test** to verify the space or percentage you entered.

Click **Save** to save the configurations and return to the Storage Configuration interface, or click **Cancel** to return to the Storage Configuration interface without saving any changes. After the physical device is saved, it will be listed in the **Physical Device** tab.

TSM

In the **Create Physical Device** or **Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device. Then, enter an optional **Description** for future reference.
2. **Storage Type** – Select **TSM** from the drop-down list.

3. **Storage Type Configuration** – Configure the following settings:

    - **Communication** – Select the protocol to use to connect to the TSM server from the drop-down menu.
    - **Server address** – Enter the host name or IP address of the TSM server.
    - **Server port** – Enter the port to use to connect to this TSM server. The default port is 1500.
    - **Node name** – Enter the name of the node you wish to connect to.
    - **Management class** – Enter the name of the management class to manage the data stored in the node.
    - **Node password** – Enter the password to use to connect to the node.

    Advanced – Enter the following extended parameters in advanced settings if necessary. Note that if you have multiple parameters to enter, press **Enter** on the keyboard to separate the parameters. Refer to the instructions below to add parameters.

        - **FileSpace** – Uses a different FileSpace under the same node. The default FileSpace is **DocAve**. Note that this parameter's value is case-sensitive. You can enter the value according to the FileSpace on your server. If the FileSpace does not exist, it will be created automatically.
        - **SingleSession** – Uses the single session for DocAve interaction with TSM Server.
            - If you enter **SingleSession=true**, it will enable the single session for DocAve interaction with TSM Server. Note that this will slow down the performance.
            - If you enter **SingleSession=false**, it will not enable the single session for DocAve interaction with TSM Server.

    Click **Validation Test** to verify that the information you entered is correct.

Click **Save** to save the configurations and return to the Storage Configuration interface, or click **Cancel** to return to the Storage Configuration interface without saving any changes. After the physical device is saved, it will be listed in the Physical Device tab.

Microsoft Azure Storage

In the **Create Physical Device** or **Edit Physical Device** interface, configure the following settings:

1. **Physical Device Name** – Enter a **Name** for this physical device. Then, enter an optional **Description** for future reference.
2. **Storage Type** – Select **Microsoft Azure Storage** from the drop-down list.
3. **Storage Type Configuration** – Configure the following settings:

    - **Access point** – Enter the URL for the Blob Storage Service. The default URL is *http://blob.core.windows.net*.

- **Container name** – Enter the **Container Name** you wish to access.
- **Account name –** Enter the corresponding **Account Name** to access the specified container.
- **Account key** – Enter the corresponding **Account key** to access the specified container.
- **CDN enabled** – Select this checkbox if the Microsoft Azure content delivery network (CDN) is enabled.
- **Advanced** – Enter the following extended parameters in **Advanced** settings if necessary. If you have multiple parameters to enter, press **Enter** on your keyboard to separate the parameters. Refer to the instructions below to add parameters.
    - **RetryInterval** – Customize the retry interval when the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646 (the unit is millisecond). For example, RetryInterval=30 represents the interval between the network interruption and reconnection is 30 milliseconds.

      If you do not configure this parameter, the value is 30 seconds by default.
    - **RetryCount** – Customize the reconnection times after the network connection is interrupted. You are allowed to enter any positive integer between 0 and 2147483646. For example, RetryCount=10 represents when the network connection is interrupted, it can reconnect at most 10 times.

      If you do not configure this parameter, the value is 6 by default.
    - **CustomizedMetadata** – Configure if DocAve customized metadata or user-added metadata is supported. By default, DocAve customized metadata and user-added metadata are all supported in DocAve.
    - **CustomizedMode=Close –** This physical device will not support DocAve customized metadata or user-added metadata.
    - **CustomizedMode=SupportAll** – This physical device will support all DocAve customized metadata and user-added metadata.
    - **CustomizedMode=DocAveOnly** – This physical device will only support DocAve customized metadata.
    - **CustomizedMode=CustomizedOnly** – This physical device will only support user-added metadata.

Click **Validation Test** to verify that the information you entered is correct.

Click **Save** to save the configurations and return to the Storage Configuration interface, or click **Cancel** to return to the **Storage Configuration** interface without saving any changes. After the physical device is saved, it will be listed in the **Physical Device** tab.

Logical Device

DocAve has the ability to treat multiple storage drives as a single logical unit when saving DocAve data. This is especially helpful for very large DocAve plans as many smaller drives can be combined. A logical drive must be defined before creating a DocAve plan.

***Note:** Each logical device can only be configured with one type of physical device.

To access **Logical Device** settings for DocAve, in the **Control Panel** interface, click **Logical Device** under the **Storage Configuration** heading. You will be brought to the **Storage Configuration** interface with the **Logical Device** tab selected. Click **Close** on the ribbon to close the **Storage Configuration** interface.

In the **Logical Device** configuration interface, you will see a list of previously configured logical devices.

Managing Logical Devices

In **Storage Configuration**, you can create a new logical device, view details about a logical device, edit a previously configured logical device, or delete a previously configured logical device. For details on creating or editing a logical device, see the Configuring Logical Devices section of this guide.

To view details about a logical device, select a logical device from the list of previously configured logical devices, and then click **View Details** on the ribbon. You will see all of the detailed information about the specific logical device displayed in the following three tabs:

- **Summary** – The configurations for this logical device.
- **Physical Device** – The physical devices that are used by this logical device.
- **Associated Storage Policy** – The storage policy that uses this logical device.

Click **Edit** on the ribbon to change the configurations for this logical device. For details on editing configurations for a logical device, see the Configuring Logical Devices section of this guide.

To delete a logical device from DocAve, select a logical device from the list of previously configured logical devices, and then click **Delete** on the ribbon. A confirmation window will pop up and ask if you are sure you want to proceed with the deletion. Click **OK** to delete the selected logical devices, or click **Cancel** to return to the **Storage Configuration** interface without deleting the selected logical devices.

***Note:** The logical device cannot be deleted if it is currently being used by one or more plans/profiles.

Configuring Logical Devices

To create a new logical device, click **Create** on the ribbon, and then select **Logical Device** from the drop-down menu. To modify a previously configured logical device, select the logical device, and then click **Edit** on the ribbon.

In the **Create Logical Device** or **Edit Logical Device** interface, configure the following settings:

1. **Logical Device Name** – Enter a **Logical device name** for this logical device. Then enter an optional **Description** for future reference.
2. **Data Storage Type** – Select the device type according to different types of the data you are about to store:

    - **Standard storage device** – This storage device can be used to store all kinds of data. It is the common type of device.
    - **BLOB storage device** – This storage device is used to store the BLOB data. It can only be used for the Storage Manager.

      ***Note:** When selecting the **BLOB storage device**, you can select the **Configure Folder Structure** feature to generate the BLOB data folders in the structure you selected.

    - **Redundant backup data storage device** – Stores the data of Platform Backup and Granular Backup.

      ***Note:** When selecting the **Redundant backup data storage device**, add two storage groups so that if the current storage group is damaged, the data can be obtained from the other storage group.

    - **Concurrent storage device** – Backs up data to the device with the optimal performance instead of the next one in the device order, which improves backup efficiency.

    ***Note:** Once the **Data Storage Type** is configured, it cannot be modified later.

3. **Storage Type** – From **Storage type** drop-down box, select the storage type for this logical device. This will determine the physical devices available to be added to this logical device. Note that when you have selected the **Blob storage device**, the **Redundant backup data storage device** and the **Concurrent storage device** as **Data Storage Type**, only the **Net Share** and **IBM Storwize Family** can be selected as **Storage Type**.
4. **Add Physical Device** – Select the physical device you wish to add from the **Physical Device** drop-down menu. You can also choose **New Physical Device** to create a new one. Click **Add** to add the physical device to this logical device. For more information on creating a new physical device, see the Configuring Physical Devices section of this guide.

    You can change the order of the physical devices by selecting a different position number in the **Order** drop-down box. The data/index will be stored in the physical device according to this order. For each physical device that you add, you may select **Data**, **Index**, or both by selecting the corresponding checkbox that you want to store in this physical device. By default, both options are selected. To remove a Physical Device, click the corresponding remove (X) button.

    Note: On the **Edit Logical Device** interface, with more than one physical device added to this logical device, if you deselect the **Data**/**Index** checkbox or remove a physical device here, a confirmation window will pop up when you click **Save** and inform you that the old backup data will be unavailable until you copy the old data/index manually to a new physical device. You have to create some folders under the path of the new physical device, with the same name and the same hierarchy as those of the old physical device, and copy the old data/index manually to

the folder with the same name and the same hierarchy as that of the old data/index. Otherwise, the old data/index cannot be found after data recovery.

When the **BLOB storage device** or the **Redundant backup data storage device** is selected in the **Storage Type** section, click the **Add a Storage Group** link in the **Add Physical Device** section to add a storage group. To add a storage group, complete the following steps:

- **Add a Storage Group** – This feature is used for the BLOB storage device and the Redundant backup data storage device. When selecting **Standard storage device** and **Concurrent storage device**, the **Add a Storage Group** link will be hidden.
- **Please choose the synchronization method for the specified storage groups** – This feature is only used for the **BLOB storage device**. When more than one storage groups have been added, this feature will be displayed. This feature allows you to enable data synchronization among several storage groups and provide high available performance to your data. This means that if the current used storage group is damaged, the data can be obtained from the other storage groups. This option is only available for **Net Share** and **IBM Storwize Family** physical devices and it is only supported for **Real-Time Storage Manager** and **Scheduled Storage Manager**. This feature will help you synchronize data to all of the storage groups. The storage groups will be used in the order that they have been added. The primary group will be used first by priority.
    - **Asynchronous** – Enables the data to be written into the first available storage group, and then DocAve will copy the successful written data from the specified storage group to all of the other storage groups.
    - **Synchronous** – Enables the data to be written into all storage groups at the same time. The synchronization thread will keep all of the data in the storage groups same, complete and correct.

5. **Configure Folder Structure** – This is an optional feature. When selecting the **BLOB storage device**, configure the **Configure Folder Structure** field to generate the BLOB data folders in the structure you selected here. After selecting the **Create storage path for contents using the following structure** checkbox, select the following radio buttons:
    - **Time and date** – Adds additional information such as modified time to the pat to make the identification of BLOBs in the storage location easier. Select one of the following four options from the drop-down list:
        - **YYYY/MM** – Select this to generate the folders. The directory of your stored data is *.../YYYY/MM*.
        - **YYYY/MM/DD** – Select this to generate the folders. The directory of your stored data is *.../YYYY/MM/DD*.
        - **YYYY/MM/DD/HH**– Select this to generate the folders. The directory of your stored data is *.../YYYY/MM/DD/HH*.
        - **YYYY/MM/DD/HH/mm** – Select this to generate the folders. The directory of your stored data is *.../YYYY/MM/DD/HH/mm*.

- **SharePoint structure** – Generates the folders to store the BLOB data according to the SharePoint hierarch of the data. This option is invalid for **Real-Time Storage Manager**.

When selecting the logical device or the backup storage device, this feature will be hidden.

6. Click **Save** to save the configurations and return to the **Storage Configuration** interface, or click **Cancel** to return to the **Storage Configuration** interface without saving any changes. After the logical device is saved, it will be listed in the **Logical Device** tab.

Storage Policy

Use **Storage Policy** to select which logical device to use when saving backup data, and setting up the retention policy for the data saving in the logical device.

To access **Storage Policy** settings, click **Storage Policy** under the **Storage Configuration** heading. You will be redirected to the **Storage Configuration** interface with the **Storage Policy** tab selected. Click **Close** on the ribbon to close the **Storage Configuration** interface.

In the **Storage Policy** configuration interface, you will see a list of storage policies.

Managing Storage Policies

In **Storage Configuration**, you can create, view details, edit or delete a storage policy. For details on creating or editing a storage policy, refer to Configuring Storage Policies.

To view details about a storage policy, select it from the list of previously configured storage policies, and then click **View Details** on the ribbon. You will see all of the detailed information about the specific storage policy displayed in the following three tabs:

- **Summary** – The configurations for this storage policy.
- **Logical Device** – The logical devices that are used by this storage policy.
- **Data** – The size of the data stored in this storage policy.

Click **Edit** on the ribbon to change the configurations for this storage policy. For more information, refer to Configuring Storage Policies.

***Note:** If the storage policy is currently being used by one or more plans, a window will pop up and ask if you are sure you want to edit this storage policy since any changes made to it will affect all of these plans.

To delete a storage policy from DocAve, select it from the list of storage policies, and then click **Delete** on the ribbon. A confirmation window will pop-up and ask if you are sure you want to proceed with the deletion. Click **OK** to delete the selected storage policies or click **Cancel** to return to the **Storage Configuration** interface without deleting the selected storage policies.

***Note:** The storage policy cannot be deleted if it is currently being used by one or more plans/profiles.

Configuring Storage Policies

To create a new storage policy, click **Create** on the ribbon, and then select **Storage Policy** from the drop-down menu. To modify a storage policy, select the storage policy, and then click **Edit** on the ribbon.

In the **Create Storage Policy** or **Edit Storage Policy** interface, configure the following settings:

1. **Storage Policy Name** – Enter a **Name** for this storage policy. Then, enter an optional **Description** for future references.
2. **Primary Storage** – Select the desired logical device from the **Logical Device** drop-down menu. The backup data will be saved in the logical device specified here. You can also choose **New Logical Device** to create a new one. For more information, refer to Configuring Logical Devices.
3. **Media Service** – Select the Media service from the drop-down menu, and then click **Add**. To remove a Media service from this storage policy, click the corresponding remove (**X**) button. Click **Test** to verify the availability of the Media services.

   If you have added several Media services, you can select the one of the following methods:

   - **Default priority** – The Media service will the most free space will be used by default.
   - **Custom priority** –Configure the positions of the Media services. The Media service with the higher priority will be used when running jobs using this storage policy.
4. **Enable Retention Rule** – To configure a retention rule for this storage policy, select the **Enable retention rule** checkbox. For more information, refer to Configuring Retention Rules.

Click **Save** to save the configurations and return to the **Storage Configuration** interface, or click **Cancel** to return to the **Storage Configuration** interface without saving any changes. After the storage policy is saved, it will be listed in the **Storage Policy** tab.

Configuring Retention Rules

After selecting the **Enable Retention Rule** option, the **Storage Policy Type** will appear. You can select **Backup type** or **Archive type** for the retention rule. After selecting the **Enable Retention Rule** option, the **Primary Retention Rule** configurations will appear. To configure settings for the **Primary Retention Rule**, follow the instructions below:

In the **Storage Policy Type** section, choose the usage of the storage policy. There are two storage policy types: **Backup type** and **Archive type**.

Backup Type

Select this to use the storage policy for the **Data Protection** modules and the **Content Manager** module. The following settings must be configured:

***Note**: One backup cycle includes a full backup job plus all incremental and differential backup jobs prior to the start of the next full backup job.

1. **Notification** – Configure e-mail notification settings for the retention jobs. You can click the checkbox and select an e-mail notification profile in the drop-down list or you can click **New Notification Profile** to set up a new e-mail notification profile. For more information about how to configure notification profiles, refer to User Notification Settings.

2. **Retention Rule** – Select one or both of the following to keep data by cycles. If both of the following two rules are selected, DocAve will keep the data specified in both of these rules:

    - **Keep the last __ cycle(s)** – Configure the number of most recent backup cycles to keep. The cycles which are older than the specified cycles will be pruned. For example, if you enter 2 here, all backup data within the last 2 full backup cycles will be kept.

      ***Note**: If you choose to trigger the data retention before the backup job starts in the **Retention Trigger Settings** section, AvePoint recommends you to keep at least 2 backup cycles to protect your backup data.

    - **Keep the last __ full backup(s)** – Configure the number of most recent full backups to keep. All of the backups which are older than the specified number of full backups will be pruned. For example, if you enter 2 here, only the latest 2 full backups will be kept. All other backups will be deleted.

      Click **Advanced If you want to keep your data by time** to access the following options for keeping data by time. If both of the following two rules are selected, DocAve will keep the data specified in both of these settings:

    - **Keep the cycle(s) in __ __ –** Keep the backup cycles within the time frame configured here. The cycles which are older than the specified time frame will be pruned. For example, if you select **Day(s)** and enter 2 here, all backup data within the full backup cycles whose start time is within the last two days will be kept.
    - **Keep the full backup(s) in __ __ –** Keep the full backups within the time frame configured here. All backup data older than the specified time frame will be pruned. For example, if you select **Day(s)** and enter 2 here, only the data of full backups whose start time is within the last two days will be kept. All older backup data will be deleted.

3. **Others** – Select the **Do not perform actions on any jobs meeting the retention rule that have stopped, failed, or finished with exception** checkbox if you do not wish to delete the backup data of the **Stopped**, **Failed**, or **Finished with Exception** jobs that meet the retention rule.

    ***Note:** If you have configured the **Advanced If you want to keep your data by time** settings, this option will be hidden.

4. **Retention Trigger Settings** – Configure the retention trigger settings. You can only configure the **Retention Trigger Settings** in the primary retention rule.

    - **Trigger data retention** – Select the **Before the backup job starts** radio button to trigger the data retention before the backup job starts. Select the **After the backup job completes** radio button to trigger the data retention after the backup job completes.

      ***Note**: If you choose to trigger the data retention before the backup job starts, AvePoint recommends you to keep at least 2 backup cycles when configuring the retention rule.

- **Select the backup types to trigger data retention** – Select the **Full backup** radio button to trigger the data retention when performing the full backup jobs. Select **Incremental backup** radio button to trigger the data retention when performing the incremental backup jobs. Select **Differential backup** radio button to trigger the data retention when performing the differential backup jobs
- **Trigger data retention when a backup is** – Select the **Finished** radio button to trigger the data retention when the backup jobs are finished. Select the **Finished with exception** radio button to trigger the data retention when the backup jobs are finished with exception.

  ***Note:** With the **Before the backup job starts** radio button selected, the **Select the backup types to trigger data retention** and **Trigger data retention when a backup is** radio buttons are invisible and data of the oldest cycle or the oldest full backup job in the configured retention rule will always be deleted, regardless of the status of the next full backup job.

5. **Action** – Configure the action you wish DocAve to perform when the retention rules are triggered:
   - **Delete the data** – Select this option to delete any data not included in the retention rule. The excluded data will be deleted when the retention job runs. To also remove related job records from **Job Monitor**, select the **Remove the job** checkbox.
   - **Move the data to logical device** – Select this option to move any data not included in the retention rule to another logical device. Then select a logical device from the drop-down menu.

     Once you have selected a logical device to move the data to, the **Secondary Retention Rule** configurations will appear. Follow the same instructions for configuring the **Primary Retention Rule**.

     ***Note:** You can have as many retention rules as the number of logical devices you have configured, and the rules are applied in order. Make sure the logical device you will move data to has enough space.

   - **Custom action** – Use your own retention policy. This function only supports storage policies for Net Share and IBM Storwize Family devices. If you create an executable file with a customized configuration, you can use it for a DocAve retention policy. Enter the local path of the executable file in the text box. For example, *C:/DocAve/policy.bat*. Click **Test** to verify the connection.

     Enter the description for the custom action in the **Description** section. The description will be shown as the warning message when the user wants to restore the data pruned by the custom action.

     ***Note:** The **Custom action** does not support the **Redundant backup data storage device**.

***Note**: The executable file is required to be able to handle two parameters: the relative path of the physical device and that of the backup data. For example, the first parameter is \\admin-PC\c$\data or \\admin-PC\shared folder, the second parameter is …\data_granular\FarmName\PlanID\CycleId\JobId.

Archive Type

Select **Archive type** to use the storage policy for the **Archiver** module. The following settings must be configured:

1. **Notification** – Configure e-mail notification settings for the retention jobs. You can click the checkbox and select an e-mail notification profile in the drop-down list or you can click **New Notification Profile** to set up a new e-mail notification profile.
2. **Schedule** – Select the date and time of day for the Start time for the archive data retention rule. Then enter a positive integer in the Interval text box for the frequency, and select either Minute(s), Hour(s) as the time unit for the interval. By default, it is 24 hours.

   ***Note:** For scheduled retention jobs, if there is no data to be pruned when the job is scheduled to run, the job will not run.

   ***Note:** Your default time zone is selected, and you may change the time zone by clicking on the hyperlink, and then selecting the desired time zone from the drop-down menu.

3. **Retention Rule** – Configure the following settings:
   - **Keep the last __ __** – Keep the archived data within the time frame configured here. For example, if you enter **2** and select **Day(s)** here, the archived data will be kept for 2 days before it is deleted by the retention job.
4. **Action** – Configure the action you wish DocAve to perform when the retention rules are triggered:
   - **Delete the data** – Select this option to delete any data not included in the retention rule. The corresponding data will be deleted when the retention job runs.
     - **Remove the job** – Removes the related job records from **Job Monitor**.
     - **Pre-scan expiring retention policies of archived data** – Generates data that is used in reports to show the scheduled deletion dates of archived content. These reports can then be attached to the e-mail notifications. You can also download the reports in **Job Monitor**.
       - **Start time** – Select the start time for the pre-scan job.
       - **Scan Interval** – Enter an interval for the pre-scan job.
       - **Include archived objects that will be pruned in __ days** – Enter a time period. The archived data which will be pruned in the specified time period will be included in pre-scan jobs and the corresponding reports.

- **Move the data to logical device** – Select this option to move any data not included in the retention rule to another logical device. Then select a logical device from the drop-down menu.

5. **Take effect on all the existing archived data** – This option will only be displayed when changing the original specified time for keeping the archived data or changing the original **Action** settings. If this option is selected, this new retention rule will take effect on all of the existing archived data; otherwise, this new retention rule will only affect the newly archived data after this retention rule configuration.

   Once you have selected a logical device to move the data to, the Secondary Retention Rule configurations will appear. Follow the same instructions for configuring the Primary Retention Rule. Note that you can have as many retention rules as the number of logical devices you have configured, and the rules are applied in order. Make sure the logical device you will move data to has enough space.

Data Manager

Use **Data Manager** to manage data and configure data settings. With this function, you can import data from DocAve, or a third party tool to DocAve 6. To access **Data Manager** for DocAve in the **Control Panel** interface, click **Data Manager** under the **Data Manager** heading in **Specific Products Settings**.

***Note**: If you are not licensed for a certain module, the corresponding button on the ribbon will be greyed out in the **Data Manager** interface.

Importing Data from DocAve 5 to DocAve 6

To configure a DocAve 5 to DocAve 6 data import, click the **DocAve 5** button on the ribbon in the **Data Manager** interface. To access the data importing configuration interface for different modules, follow the instructions in the sections below for each module in the **Data Manager** interface. You can also click **Data Type** on the ribbon and select the data you want to process from the drop-down list.

***Note**: DocAve 6 now supports data imports from DocAve version 5.5 to DocAve version 5.8. If you want to import data from DocAve 5 to DocAve 6 and are using a DocAve version lower than 5.7, it is recommended that you upgrade to version 5.7 first and then import your data from DocAve 5.7 to DocAve 6.

***Note**: To guarantee the success of the data import from DocAve 5 to DocAve 6, you must go the Scheduled Job Monitor in DocAve 5 to stop all of the scheduled jobs.

Importing DocAve 5 Granular Backup Data

Before you begin, you must configure a storage policy and a logical device. To configure a storage policy, open the Control Panel interface and click the **Storage Policy** link under the Storage Configuration category in Specific Products Settings. Then create a storage policy with a logical device pointing to the

DocAve 5 Granular Backup Data and Index locations. For details on configuring the storage policy, refer to the Configuring Storage Policies section of this user guide.

To configure a logical device, go to the Control Panel Interface and click the **Logical Device** link under the Storage Configuration category in Specific Products Settings. Then create a logical device with a physical device pointing to the DocAve 5 Granular Backup Data and Index location. For details on configuring the logical device, refer to the Configuring Logical Devices section of this user guide.

When setting up the DocAve 6 physical devices, make sure you are using the same path and settings as the DocAve 5 physical devices.

After you finish your configurations, return to the **Control Panel** and click the **Data Manager** link under the **Data Manager** category in **Specific Products Settings**. From the **Data Manager** interface, click the **Data Type** button on the ribbon, and then select **Granular Backup Data** from the drop-down list.

***Note**: DocAve does not support the upgrade of Granular Backup data stored on the **DELL DX Storage** and **EMC Centera** storage.

To import DocAve 5 Granular Backup Data to DocAve 6, complete the following steps:

1. **Prerequisite** – Have you mapped the device storing DocAve 5 granular backup data to a DocAve 6 storage policy?
    - If you already configured a storage policy according to the directions at the start of this section, and then select **Mapped**. Click **Next** to go to the next step.
    - If you have not completed these configurations, select **Not mapped** (the default selection), and then click the **Configure Storage Policy** link. Complete your storage policy configurations, and return to the Prerequisites page. Select **Mapped**, and click **Next** to go to the next step.
2. **Data Selection** – Select the data you want to import from DocAve 5. In the **Storage Policy** drop-down list, select a storage policy that you previously configured. In the tree, you can browse from farm level to full backup cycle level. If you want to import data of a farm, select the **Select All** checkbox under the farm name. You can also separately select the backup job you want to include. Click **View Details** to view the logical device that will be used for this backup job and all of the jobs in the cycle. If you check a previously imported backup job, you can view the last imported time in the **Last Imported Time** column.

    ***Note:** If you want to import the previously imported backup data and there is no logical device change or new job in the cycle added, the job data importing job will skip. In the comment column of Job Monitor, it displays: **The job's data has existed**.

    After you finish the configuration, click **Next** to go to the next step.
3. **Notification** – Send out an e-mail notification report to specified DocAve users. In the **Select a profile with address only** drop-down list, select the e-mail notification you previously configured. You can also click **New Notification Profile** to create a notification. Click **View** to see the **User Notification Settings** window. You can view the detailed setting of the notification

here. Click **Edit** to edit the notification setting or click **Close** to close the window. After you finish the configuration, click **Next** to go to the next step.

4. **Overview** – Review your configurations. In the **Imported Plans and Settings** table, you can view the detailed information of the DocAve 5 Granular Backup Data import. During the setting, you can click **Back** to go to a previous step or click **Cancel** to exit the configuration GUI.
5. Click **Finish** to save the configuration and return to the Data Manger GUI, or click **Cancel** to return without saving any changes. You can click **Job Monitor** on the ribbon to go to the Job Monitor GUI and view the job detail.

Importing DocAve 5 Platform Backup Data

Before you begin, you must configure a storage policy and a logical device. To configure a storage policy, open the Control Panel interface and click the **Storage Policy** link under the Storage Configuration category in Specific Products Settings. Then create a storage policy with a logical device pointing to the DocAve 5 Platform Backup Data and Index location. For details on configuring the storage policy, refer to the Configuring Storage Policies section of this user guide.

To configure a logical device, go to the Control Panel Interface and click the **Logical Device** link under the Storage Configuration category in Specific Products Settings. Then create a logical device with a physical device pointing to the DocAve 5 Platform Backup Data and Index location. For details on configuring the logical device, refer to the Configuring Logical Devices section of this user guide.

When setting up the DocAve 6 physical devices, make sure you are using the same path and settings as the DocAve 5 physical devices.

After you finish your configurations, return to the Control Panel and click the **Data Manager** link under the Data Manager category in Specific Products Settings. From the Data Manager interface, click the **Data Type** button on the ribbon, and then select **Platform Backup Data** from the drop-down list.

***Note**: DocAve does not support the upgrade of Platform Backup data stored on the **EMC Centera** storage.

Complete the following steps to import DocAve 5 Platform Backup Data to DocAve 6:

1. **Prerequisites** – Have you mapped the device storing DocAve 5 platform backup data to a DocAve 6 storage policy?
    - If you already configured a storage policy according to the directions at the start of this section, and then select **Mapped**. Click **Next** to go to the next step.
    - If you have not completed these configurations, select **Not mapped** (the default selection), and then click the **Configure Storage Policy** link. Complete your storage policy configurations, and then return to the Prerequisites page. Select **Mapped**, and click **Next** to go to the next step.
2. **Data Selection** – Select the data you want to import from DocAve 5. On the **Storage Policy** drop-down list, select a storage policy that you previously configured. In the tree, you can browse

from agent level to full backup cycle level. If you want to import data run by a certain agent, select the **Select All** checkbox under the agent name. You can also separately select the backup job you want to include. Click **View Details** and you can view the logical device that will be used for this backup job and all of the jobs in the cycle. If you check a previously imported Platform Backup job, you can view the last imported time in the **Last Imported Time** column.

After you finish the configuration, click **Next** to go to the next step.

3. **Notification** – Send out an e-mail notification report to specified DocAve users. In the **Select a profile with address only** drop-down list, select the e-mail notification you previously configured. You can also click **New Notification Profile** to create a notification. Click **View** to see the User Notification Settings window. You can view the detailed setting of the notification here. Click **Edit** to edit the notification setting or click **Close** to close the window. After you finish the configuration, click **Next** to go to the next step.
4. **Overview** – Review your configurations. In the **Imported Plans and Settings** table, you can view the detailed information of the DocAve 5 Platform Backup Data import. During the setting, you can click **Back** to go to a previous step or click **Cancel** to exit the configuration GUI.
5. Click **Finish** to save the configuration and return to the Data Manger GUI, or click **Cancel** to return without saving any changes. You can click **Job Monitor** on the ribbon to go to Job Monitor GUI and view the job detail.

Importing DocAve 5 Archiver Data

Before you begin, you must configure a logical device and a storage policy. To configure a logical device, go to the Control Panel Interface and click the **Logical Device** link under the Storage Configuration category in Specific Products Settings. Then create a logical device with a physical device pointing to the DocAve 5 Archiver Index location. For details on configuring the logical device, refer to the Configuring Logical Devices section of this user guide.

From the Control Panel interface, click the **Storage Policy** link under the Storage Configuration category in Specific Products Settings. Then create a storage policy with a logical device pointing to the DocAve 5 Archiver Data location. For details on configuring the storage policy, refer to the Configuring Storage Policies section of this user guide.

When setting up the DocAve 6 physical devices, make sure you are using the same path and settings as the DocAve 5 physical devices.

After you finish configuring the logical device and the storage policy, return to the Control Panel and click the **Data Manager** link under the Data Manager category in Specific Products Settings. From the Data Manager interface, click the **Data Type** button on the ribbon, and then select **Archiver Data** from the drop-down list.

***Note**: This importing option is used for DocAve 5 Archiver data which has no DocAve 5 Archiver stubs created.
***Note**: DocAve does not support the upgrade of Archiver data stored on the **DELL DX Storage** and **EMC Centera** storage.

Complete the following steps to import DocAve 5 Archiver Data to DocAve 6:

1. **Prerequisites** – Have you completed the following mappings and configurations?

    - **Have you mapped the DocAve 5 Archiver index to a DocAve 6 logical device** – You must configure a logical device with a physical device pointing to the DocAve 5 Archiver Index Location. For details about how to configure a logical device, refer to Configuring Logical Devices section in this user guide.

        - If you already configured a logical device according to the directions at the start of this section, and then select **Mapped**.

        - If you have not completed these configurations, select **Not mapped** (the default selection), and then click the **Configure Logical Device** link. Complete your logical device configuration, and then return to the Prerequisites page, and select **Mapped**.

    - **Have you mapped the DocAve 5 Archiver data device to a DocAve 6 storage policy?** – You must configure a storage policy with a physical device pointing to the DocAve 5 Archiver Data location. For details about how to configure storage policy, refer to Configuring Storage Policies.

        - If you already configured a physical device according to the directions at the start of this section, and then select **Mapped**.

        - If you have not completed these configurations, select **Not mapped** (the default selection), and then click the **Configure Storage Policy** link. Complete your logical device configuration, and then return to the Prerequisites page, and select **Mapped**.

    - **Have you configured a DocAve 6 Archiver index device** – You must configure an Archiver Index Device to store DocAve 6 Archiver index.

        - If you have already configured the Archiver Index Device, select **Configured**.

        - If you have not configured the Archiver Index Device, click the **Configure Archiver Index Device** link to enter the Configure Archiver Index Device interface. Complete the Archiver Index Device configuration, and then return to the Prerequisites page, and select **Configured**.

    Once you have selected **Mapped** or **Configured** for all three fields, click **Next** to go to the next step.

2. **Data Selection** – Select the Archiver index you want to import from DocAve 5. On the Device drop-down list, select the DocAve 6 logical device you previously configured for mapping the DocAve 5 Archiver index. In the tree, you can browse from farm level to site collection level and select the level you want to import index from. If you check a previously imported level, you can view the last imported time of the index in the **Last Imported Time** column. If you want to import the index you imported before, you can select the same data level, and after the job completes, the last imported time will change to the latest time. After you finish the configuration, click **Next** to go to the next step.

3. **Settings** – Configure the following settings:

- **Media Service** – Select a media service to get the Index data from DocAve 5. Click the drop-down list, and select the media service you want for the index import.
- **Notification** – Select a notification profile to send out an e-mail notification report to specified DocAve users. You can select a previously configured notification profile in the drop-down list or click **New Notification Profile** to create a new notification profile. For details on how to configure a notification setting, refer to the User Notification Settings section in this user guide.
- **Pre-scan** – Scan your device mapping status for the DocAve 5 Archiver data before running an import job. Select **Scan the device mapping status before importing DocAve 5 Archiver index and data**. DocAve will run the following two jobs: **Archiver Scan Data** job and **Archiver Import Data** job. This will make sure that all of your DocAve 5 Archiver Data devices in the scope specified in the **Data Selection** step have been mapped to the corresponding DocAve 6 storage policy.

4. Click **Finish** to save the configuration and return to the Data Manger GUI, or click **Cancel** to return to the Data Manager GUI without saving any changes. You can click **Job Monitor** on the ribbon to go to Job Monitor GUI and view the job details.

Converting DocAve 5 Stubs and BLOB Data

Before you can convert DocAve 5 stubs and BLOB data, you must configure the BLOB Provider and a logical device. From the Data Manager interface in Control Panel, click the **Blob Provider** link in the **Archiver/Extender Stub and BLOB Data** field to configure the BLOB provider settings. For details on how to set up the BLOB Provider, refer to the Configuring the BLOB Provider section in the Storage Manager User Guide.

To select a logical device to store the BLOB data which is imported from DocAve 5, go to Control Panel and click the **Logical Device** link under the Storage Configuration heading in Specific Products Settings. For details on configuring the logical device, refer to the Configuring Logical Devices section of this user guide.

After you finish these configurations, return to the Control Panel. Then click the **Data Manager** link under the Data Manager category in Specific Products Settings. Click the **Data Type** button on the ribbon, and then select **Archiver/Extender Stub and Blob Data** from the drop-down list.

Complete the following steps to configure the stub and BLOB data import:

1. **Prerequisites** – Have you completed the following configurations?
    - **BLOB Provider** – You must configure the BLOB Provider in Storage Optimization before you can continue:
        - If you already configured the BLOB Provider according to the directions at the start of this section, and then select **Configured**.
        - If you have not completed this configuration, select **Not Configured** (the default selection), and then click the **Configure Blob Provider** link. Complete your BLOB

Provider configuration, and then return to the Prerequisites page, and select **Configured**.

- **Configure Logical Device** – You must configure a logical device for storing the imported DocAve 5 BLOB data.
    - If you already configured a logical device according to the directions at the start of this section, and then select **Configured**.
    - If you have not completed this configuration, select **Not Configured** (the default selection), and then click the **Configure Logical Device** link. Complete your logical device configuration, and then return to the Prerequisites page, and select **Configured**.

Once you have selected **Configured** for both fields, click **Next** to go to the next step.

2. **Data Selection** – Select the data you want to import from DocAve 5 in this step.
    - **SharePoint Environment** – Browse from farm level to site collection level and select the level you want to import data from. Refer to the information below for selecting nodes on the farm tree.
        - You can only select nodes in the same farm.
        - When selecting the farm, Web application, or content database, there will be a **Configure** button on the right. Note that this button is only for configuring the Storage Manager logical device for the current level you select. While the **Configure** button on the ribbon will configure the Storage Manager device for all of the selected nodes. After clicking the **Configure** button next to the node or the **Configure** button on the ribbon, select a logical device from the drop-down list or create a logical device by clicking **New Logical Device**. Click **Save** to finish the logical device configuration and go back to the Data Selection interface or click **Cancel** to exit the interface.

      ***Note:** In **Recycle Bin**, the DocAve 5 stubs in the deleted lists/libraries level or the above level will not be upgraded to the DocAve 6 stubs.

    - **Logical Device** – After you have configured the logical device, this column will show the Storage Manager logical device that you have configured.
    - **Last Imported Time** – If you checked the previously converted data in farm, Web application or content database, you can view the last imported time of the data in this column. If you want to import the data you imported before, you can select the same data level, and after the job finished, the last imported time will change to the latest time.

    After you finish the configuration, click **Next** to go to the next step.

3. **Data Settings** – Set up the following configurations:
    - **Storage Manager Settings** – In this field, you can set up Compression and Encryption for Storage Manager.

- **Data Compression** – This option allows you to compress BLOB data and save space. Select the **Compression** option and select a compression level. A low compression level results in a faster compression rate but a larger data set, while a high compression level results in a slower compression rate but a smaller, better quality data set. Note that small data sets occupy more system resources and cause slower job times. The compression is performed on the SharePoint Server (SharePoint Agent).
- **Data Encryption** – If you want to enable data encryption, check **Encryption** and select a security profile in the **Security Profile** drop-down list. You can also click **New Security Profile** to create a new security profile. Encryption protects sensitive materials; however, note that encrypting data causes slower extend times. The encryption is performed on the SharePoint Server (SharePoint Agent).

- **Agent Group** – If you have several agent groups under one farm, you can select an agent group to run the data importing job.
- **Notification** – Select a notification profile to send out an e-mail notification report to specified DocAve users. You can select previously configured notification profile in the drop-down list or click **New Notification Profile** to create a new notification profile. For details on how to configure a notification setting, refer to the User Notification Settings section in this user guide.
- **Schedule Selection** – Set up a schedule to run the converting data job. If you want to run the job right now, select **Import once finish the wizard**. If you want to set up a schedule, select **Configure the schedule myself** to have DocAve run the converting job at a designated time. You can select the start time for the job by selecting a time from the drop-down list for date and entering hour and minute in the other two text boxes.
- **Remaining DocAve 5 Stubs –** Choose whether to scan for remaining DocAve 5 stubs after importing DocAve 5 stubs to DocAve 6 by selecting or deselecting the **Scan the specified scope and report the number of remaining DocAve 5 stubs after the import** checkbox. You can view the number of remaining DocAve 5 stubs in the job report downloaded from Job Monitor. If you want to view the detailed information of the remaining DocAve 5 stubs, run the **SP2010StorageUpgradeStub** tool to obtain the details. For more information, refer to the DocAve Tools User Guide.

4. Click **Finish** to save the configuration and return to Data Manger GUI, or click **Cancel** to return to Data Manager GUI without saving any changes. You can click **Job Monitor** on the ribbon to go to Job Monitor GUI and view the job detail.

Converting DocAve 5 Connector Stub

Before you can import the Connector stubs, you must first retract and remove the DocAve 5 Connector solutions (**DocAve.SP2010.Connector. ContentLibrary.wsp** and **DocAve.SP2010.Connector.MediaLibrary.wsp**) from SharePoint, and then deploy the DocAve 6 Connector solutions (**SP2010ConnectorContentLibrary.wsp** and **SP2010ConnectorMediaLibrary.wsp**) to SharePoint. For details on how to deploy solutions for DocAve 6 Connector, refer to Solution Manager. The solutions can be deployed at farm level or Web application level in DocAve Solution Manager.

Before you can import DocAve 5 Connector stubs, you must configure the BLOB Provider. From the Data Manager interface in Control Panel, click the **Blob Provider** link in the **Connector Stub** field to configure the BLOB provider settings. For details on how to set up the BLOB provider, refer to Configuring the BLOB Provider section in the Connector User Guide.

After you finish these configurations, return to the Control Panel, click the **Data Manager** link under the Data Manager category in Specific Products Settings. Click the **Data Type** button on the ribbon, and then select **Connector Stub** from the drop-down list.

Complete the following steps to configure the DocAve Connector stubs:

1. **Prerequisites** – Have you completed the following configuration?
    - **BLOB Provider** – You must configure the BLOB Provider in Storage Optimization before you can continue:
        - If you already configured the BLOB Provider according to the directions at the start of this section, and then select **Configured**. Click **Next** to go to the next step.
        - If you have not completed this configuration, select **Not Configured** (the default selection), and then click the **Configure Blob Provider** link. Complete your BLOB Provider configuration, and then return to the Prerequisites page. Select **Configured**, and then click **Next** to go to the next step.
2. **Data Selection** – Select the Connector stub you want to import from DocAve 5.
    - **SharePoint Environment** – Browse from the farm level to the content database level and select the level you want to import Connector stub from.
    - **Last Imported Time** – If you checked the previously converted data in the farm, Web application or content database, you can view the last imported time of the data in this column. If you want to import the data imported before, you can select the same data level, and after the job finished, the last imported time will change to the latest time.
3. **Data Settings** – Set up the following configurations:
    - **Agent Group** – If you have several agent groups under one farm, you can select an agent group to run the Connector stub import job.
    - **Notification** – Select a notification profile to send out an e-mail notification report to specified DocAve users. You can select a previously configured notification profile in the drop-down list, or click **New Notification Profile** to create a new notification profile. For details on how to configure a notification setting, refer to the User Notification Settings section in this user guide.
    - **Schedule Selection** – Set up a schedule to run the converting data job. If you want to run the job right now, select **Import once finish the wizard**. If you want to set up a schedule, select **Configure the schedule myself** to have DocAve run a converting job at a designated time. You can select the start time for the job by selecting time from the drop-down list for date and entering hour and minute in the other two text boxes.

- **Remaining DocAve 5 Stubs –** Choose whether to scan for remaining DocAve 5 stubs after importing DocAve 5 Connector stubs to DocAve 6 by selecting or deselecting the **Scan the specified scope and report the number of remaining DocAve 5 stubs after the import** checkbox. You can view the number of remaining DocAve 5 stubs in the job report downloaded from Job Monitor. If you want to view the detailed information of the remaining DocAve 5 stubs, run the **SP2010StorageUpgradeStub** tool to obtain the details. For more information, refer to DocAve Tools User Guide.

4. Click **Finish** to save the configuration and return to Data Manger GUI, or click **Cancel** to return to Data Manager GUI without saving any changes. You can click **Job Monitor** on the ribbon to go to Job Monitor GUI and view the job detail.

Importing DocAve 5 Solution Data

Before you begin, you must configure a storage policy and a logical device. To configure a storage policy, open the Control Panel interface and click the **Storage Policy** link under the Storage Configuration category in Specific Products Settings. Then create a storage policy with a logical device pointing to the DocAve 5 Solution Data platform. For details on configuring the storage policy, refer to the Configuring Storage Policies section of this user guide.

To configure a logical device, go to the Control Panel Interface and click the **Logical Device** link under the Storage Configuration category in Specific Products Settings. Then create a logical device with a physical device pointing to the DocAve 5 Solution Data platform. For details on configuring the logical device, refer to the Configuring Logical Devices section of this user guide.

After you finish configuring the storage policy and logical device, return to the Control Panel and click the **Data Manager** link under the Data Manager category in Specific Products Settings. From the Data Manager interface, click the **Data Type** button on the ribbon, and then select **Solution Data** from the drop-down list.

***Note:** If you have exported DocAve 5 Solution Data and you want to upgrade the data to DocAve 6, you can use DocAve 5 Solution Data Importing to upgrade the solution data. For details on how to export DocAve 5 Solution Data, refer to the Solution Center section in DocAve 5 User Guide.

To configure the DocAve 5 Solution Data import, complete the following steps:

1. **Prerequisites** – Have you mapped the DocAve 5 Solution Center device to a DocAve 6 storage policy?

    - If you already configured a storage policy and logical device according to the directions at the start of this section, and then select **Mapped**. Click **Next** to go to the next step.
    - If you have not completed these configurations, select **Not mapped** (the default selection), and then click the **Configure Storage Policy** link. Complete your storage policy and logical device configurations, and then return to the Prerequisites page. Select **Mapped**, and then click **Next** to go to the next step.

2. **Data Selection** – Select the solution data you want to import from DocAve 5. In the **Storage Policy** drop-down list, select a storage policy you previously configured. In the tree, the root

node is the logical device's name. Click the logical device and you can browse the solutions data stored in the device.

After you finish the configuration, click **Next** to go to the next step.

3. **Notification** – Select a notification profile to send out an e-mail notification report to specified DocAve users. You can select a previously configured notification profile in the drop-down list, or click **New Notification Profile** to create a new notification profile. For details on how to configure a notification setting, refer to the User Notification Settings section in this user guide. Click **View** to view the details of the notification you selected.

   After you finish the configuration, click **Next** to go to the next step.

4. Click **Finish** to save all of the changes and go back to Data Manger GUI, or click **Cancel** to exit the configuration interface without saving any changes. A prompt message appears.
5. Click **Job Monitor** on the message to go to Job Monitor GUI and view the job details.

Importing Data from DocAve 6 to DocAve 6 Service Pack 1 or Later Versions

To configure DocAve 6 to DocAve 6 Service Pack 1 or later versions data import, click the **DocAve 6** button on the ribbon in the Data Manager GUI. To access the data importing configuration interface for different modules, follow the instructions in the sections below for each module in the Data Manager interface. You can also click **Data Type** on the ribbon and select the data you want to process from the drop-down list.

***Note**: DocAve 6 Service Pack 1 only supports the upgrade for DocAve 6 data stored on **Net Share**, **FTP**, **TSM** and **Cloud Storage**.

Importing DocAve 6 Granular Backup Data

Before you begin, you must configure a storage policy and a logical device. To configure a storage policy, open the Control Panel interface and click the **Storage Policy** link under the Storage Configuration category in Specific Products Settings. Then create a storage policy with a logical device pointing to the DocAve 6 Granular Backup Data and Index locations. For details on configuring the storage policy, refer to the Configuring Storage Policies section of this user guide.

To configure a logical device, go to the Control Panel Interface and click the **Logical Device** link under the Storage Configuration category in Specific Products Settings. Then create a logical device with a physical device pointing to the DocAve 6 Granular Backup Data and Index location. For details on configuring the logical device, refer to the Configuring Logical Devices section of this user guide.

When setting up the physical devices for DocAve 6 Service Pack 1 or later versions, make sure you are using the same path and settings as the DocAve 6 physical devices.

After you finish your configurations, return to the Control Panel and click the **Data Manager** link under the Data Manager category in Specific Products Settings. From the Data Manager interface, click the **DocAve 6** button on the ribbon, click the **Data Type**, and then select **Granular Backup Data** from the drop-down list.

1. **Prerequisites** – Have you mapped the device storing DocAve 6 granular backup data to a DocAve 6 storage policy?
    - If you already configured a storage policy and logical device according to the directions at the start of this section, and then select **Mapped**. Click **Next** to go to the next step.
    - If you have not completed these configurations, select **Not mapped** (the default selection), and then click the **Configure Storage Policy** link. Complete your storage policy configurations, and then return to the Prerequisites page. Select **Mapped**, and click **Next** to go to the next step.
2. **Data Selection** – Select the data you want to import from DocAve 6. On the **Storage Policy** drop-down list, select a storage policy that you previously configured. In the tree, you can browse from farm level to full backup cycle level. If you want to import data of a farm, check **Select All**

box under the farm name. You can also separately select the backup job you want. Click **View Details** to view the logical device that will be used for this backup job and all of the jobs in the cycle. If you check a previously imported backup job, you can view the last imported time in the **Last Imported Time** column.

***Note**: If you want to import the previously imported backup data and there is no logical device change or new job in the cycle added, the job data importing job will skip. In the comment column of Job Monitor, it displays: **The job's data has existed**.

After you finish the configuration, click **Next** to go to the next step.

3. **Notification** – Send out an e-mail notification report to specified DocAve users. In the **Select a profile with address only** checkbox, click the drop-down list and select the e-mail notification you previously configured. You can also click **New Notification Profile** to create a notification. Click **View** and a User Notification Settings window will appear. You can view the detailed setting of the notification here. Click **Edit** to edit the notification setting or click **Close** to close the window. After you finish the configuration, click **Next** to go to the next step.
4. **Overview** – Review your configurations. In the **Imported Plans and Settings** table, you can view the detailed information of the DocAve 6 Granular Backup Data import. During the setting, you can click **Back** to go to the previous step or click **Cancel** to exit the configuration GUI.
5. Click **Finish** button to save the configuration and return to Data Manger GUI or click **Cancel** to return to Data Manager GUI without saving any changes. You can click **Job Monitor** on the ribbon to go to the Job Monitor GUI and view the job detail.

Importing DocAve 6 Platform Backup Data

Before you begin, you must configure a storage policy and a logical device. To configure a storage policy, open the Control Panel interface and click the **Storage Policy** link under the Storage Configuration category in Specific Products Settings. Then create a storage policy with a logical device pointing to the DocAve 6 Platform Backup Data and Index location. For details on configuring the storage policy, refer to the Configuring Storage Policies section of this user guide.

To configure a logical device, go to the Control Panel Interface and click the **Logical Device** link under the Storage Configuration category in Specific Products Settings. Then create a logical device with a physical device pointing to the DocAve 6 Platform Backup Data and Index location. For details on configuring the logical device, refer to the Configuring Logical Devices section of this user guide.

When setting up the physical devices for DocAve 6 Service Pack 1 or later versions, make sure you are using the same path and settings as the former DocAve 6 physical devices.

After you finish your configurations, return to the Control Panel and click the **Data Manager** link under the Data Manager category in Specific Products Settings. From the Data Manager interface, click the **DocAve 6** button on the ribbon, and then click the link for **Platform Backup Data** in the Data Manager GUI.

Complete the following steps to import DocAve 6 Platform Backup Data to DocAve 6 Service Pack 1 or later versions:

1. **Prerequisites** – Have you mapped the device storing DocAve 6 platform backup data to a DocAve 6 storage policy?

    - If you already configured a storage policy according to the directions at the start of this section, then select **Mapped**. Click **Next** to go to the next step.
    - If you have not completed these configurations, select **Not Mapped** (the default selection), click the **Configure Storage Policy** link, complete your storage policy configurations, and then return to the Prerequisites page. Select **Mapped**, and then click **Next** to go to the next step.

    After you finish the configuration, click **Next** to go to the next step.

2. **Data Selection** – Select the data you want to import from DocAve 6 in this step. On the **Storage Policy** drop-down list, select a storage policy you previously configured for DocAve 6 Platform Backup data. On the tree, you can browse from farm level to full backup cycle level. If you want to import data of a farm, check **Select All** box under the farm name. You can also select the backup job you want to import separately. Click **View Details** and you can view the logical device that will be used for this backup job and all of the jobs in the cycle. If you check a previously imported Platform Backup job, you can view the last imported time in the **Last Imported Time** column.

    After you finish the configuration, click **Next** to go to the next step.

3. **Notification** – Send out an e-mail notification report to specified DocAve users. In the **Select a profile with address only** checkbox, click the drop-down list and select the e-mail notification you previously configured. You can also click **New Notification Profile** to create a notification. Click **View** to view and a **User Notification Settings** window will appear. You can view the detailed setting of the notification here. Click **Edit** to edit the notification setting or click **Close** to close the window.

    After you finish the configuration, click **Next** to go to the next step.

4. **Overview** – Review your configurations. In the Imported Plans and Settings table, you can view the detail information of the DocAve 6 Platform Backup Data importing. During the setting, you can click **Back** to go to the previous step or click **Cancel** to exit the configuration GUI.
5. Click **Finish** to save the configuration and return to the Data Manger GUI or click **Cancel** to return to Data Manager GUI without saving any changes. You can click **Job Monitor** on the ribbon to go to Job Monitor GUI and view the job detail.

    ***Note:** If the BLOB data were backed up by the Platform backup job, the value of the **Size** column in the **Job Details** interface doesn't include the size of the BLOB data.

    ***Note:** The value of the **Farm** column in the **Job Details** interface is used to distinguish the platform data and the VM data backed up by the Platform backup job. It's the platform data if the value is the farm name, while it's the VM data if the value is N/A.

Importing DocAve 6 VM Backup Data

Before you begin, you must configure a storage policy and a logical device. To configure a storage policy, open the Control Panel interface and click the **Storage Policy** link under the Storage Configuration category in the Specific Products Settings. Then, create a storage policy with a logical device pointing to the DocAve 6 VM Backup Data and Index location. For details on configuring the storage policy, refer to the Configuring Storage Policies section of this user guide.

To configure a logical device, go to the Control Panel Interface and click the **Logical Device** link under the Storage Configuration category in the Specific Products Settings. Then, create a logical device with a physical device pointing to the DocAve 6 VM Backup Data and Index location. For details on configuring the logical device, refer to the Configuring Logical Devices section of this user guide.

When setting up the physical devices, make sure you are using the same path and settings as the former DocAve 6 physical devices.

After you finish your configurations, return to the Control Panel and click the **Data Manager** link under the Data Manager category in the Specific Products Settings. From the Data Manager interface, click the **DocAve 6** button on the ribbon, and then click the link for **VM Backup Data** in the Data Manager GUI.

Complete the following steps to import DocAve 6 VM Backup Data to DocAve 6 Service Pack 5 or later versions:

1. **Prerequisites** – Have you mapped the device storing DocAve 6 VM backup data to a DocAve 6 storage policy?

    - If you already configured a storage policy, select **Mapped**. Click **Next** to go to the next step.
    - If you have not completed these configurations, select **Not Mapped** (the default selection), click the **Configure Storage Policy** link, complete your storage policy configurations, and then return to the Prerequisites page. Select **Mapped**, and then click **Next** to go to the next step.

    After you finish the configuration, click **Next** to go to the next step.

2. **Data Selection** – Select the data you want to import from DocAve 6 in this step. On the **Storage Policy** drop-down list, select a storage policy for the DocAve 6 VM Backup data. On the tree, you can browse from plan level to full backup cycle level. If you want to import data of all of the plans, check **Select All** box. You can also select the backup job you want to import separately. Click **View Details** and you can view the logical device that will be used for this backup job and all of the jobs in the cycle. If you check a previously imported VM Backup job, you can view the last imported time in the **Last Imported Time** column.

    After you finish the configuration, click **Next** to go to the next step.

3. **Notification** – Send out an e-mail notification report to specified DocAve users. In the **Select a profile with address only** checkbox, select the e-mail notification from the drop-down list. You can also click **New Notification Profile** to create a notification. Click **View** to view and a **User**

Notification Settings window will appear. You can view the detailed setting of the notification here. Click **Edit** to edit the notification setting or click **Close** to close the window.

After you finish the configuration, click **Next** to go to the next step.

4. **Overview** – Review your configurations. In the Imported Plans and Settings table, you can view the detailed information of the DocAve 6 VM Backup Data you are importing. From this page, you can click **Back** to go to the previous step or click **Cancel** to exit the configuration GUI.
5. Click **Finish** to save the configuration and return to the Data Manger GUI or click **Cancel** to return to Data Manager GUI without saving any changes. You can click **Job Monitor** on the ribbon to go to Job Monitor GUI and view the job detail.

Converting EBS Stubs to RBS Stubs in DocAve 6

If you have EBS stubs in the DocAve 6 environment and you want to convert EBS stubs to RBS stubs, this function allows you to achieve the stub converting.

To access the DocAve 6 upgrading EBS to RBS Stub configuration interface, go to the Control Panel and click the **Data Manager** link under the Data Manager category in Specific Products Settings. Then click the **RBS Blob Provider** link in the middle of the Data Manager interface. You must enable RBS for the farm, Web application, or content database you want to convert to RBS stubs. For details on how to enable RBS, refer to the Configuring the BLOB Provider section in the Storage Manager User Guide.

After you finish these configurations, return to the Data Manager interface. Click the **DocAve 6** button on the ribbon, click the **Data Type** button, and then select **EBS to RBS Stub** from the drop-down list.

To configure the stub converting, complete the following steps:

1. **Data Selection** – Select a farm for the DocAve 6 EBS stubs converting. On the Farm Selection drop-down list, select a farm you want to convert EBS stubs. Click **Next** to go to the next step.

   ***Note**: All EBS rules and the EBS provider of the selected farm will be disabled after the converting job finishes.

2. **Data Settings** – Set up the following configurations:

   - **Agent Group** – If you have several agent groups under one farm, you can select an agent group to run the EBS stub converting job.
   - **Notification** – Select a notification profile to send out an e-mail notification report to specified DocAve users. You can select a previously configured notification profile in the drop-down list or click **New Notification Profile** to create a new notification profile. For details on how to configure a notification setting, refer to the User Notification Settings section in this user guide.

3. **Schedule Selection** – Set up a schedule to run the converting data job. If you want to run the job right now, select **Start converting once finish the wizard**. If you want to set up a schedule, select **Configure the schedule myself** to have DocAve run the converting job at a designated time. You

can select the start time for the job by selecting time from the drop-down list for the date and entering hour and minute in the other two text boxes.

4. Click **Finish** to save the configuration and return to Data Manger GUI or click **Cancel** to return to Data Manager GUI without saving any changes. You can click **Job Monitor** on the ribbon to go to Job Monitor GUI and view the job detail.

Importing DocAve 6 SharePoint Migration Data

Before you begin, you must configure a storage policy and a logical device. To configure a storage policy, open the **Control Panel** interface and click the **Storage Policy** link under the **Storage Configuration** category in Specific Products Settings. Then create a storage policy with a logical device pointing to the DocAve 6 SharePoint migration exported data location. For details on configuring the storage policy, refer to the Configuring Storage Policies section of this user guide.

To configure a logical device, go to the **Control Panel** Interface and click the **Logical Device** link under the **Storage Configuration** category in Specific Products Settings. Then create a logical device with a physical device pointing to the DocAve 6 SharePoint migration exported data location. For details on configuring the logical device, refer to the Configuring Logical Devices section of this user guide.

When setting up the physical devices for DocAve 6 Service Pack 3 or later versions, make sure you are using the same path and settings as the former DocAve 6 physical devices.

After you finish your configurations, return to the **Control Panel** interface and click the **Data Manager** link under the **Data Manager** category in Specific Products Settings. From the **Data Manager** interface, click the **DocAve 6** button on the ribbon, and then click **SharePoint Migration** data link in the Data Manager GUI.

Complete the following steps to import DocAve 6 SharePoint Migration exported data to DocAve 6 Service Pack 3 or later versions:

1. **Prerequisites** – Have you mapped the device storing DocAve 6 SharePoint Migration data to a DocAve 6 storage policy?

    - If you already configured a storage policy according to the directions at the start of this section, and then select **Mapped**. Click **Next** to go to the next step.
    - If you have not completed these configurations, select **Not mapped** (the default selection), click the **Configure Storage Policy** link, complete your storage policy configurations, and then return to the **Prerequisites** page. Select **Mapped**, and then click **Next** to go to the next step.

    After you finish the configuration, click **Next** to go to the next step.

2. **Data Selection** – Select the data you want to import from DocAve 6 in this step. On the **Storage Policy** drop-down list, select a storage policy you previously configured for DocAve 6 SharePoint Migration exported data. On the tree, you can browse from farm level to full backup cycle level. If you want to import data of a farm, check **Select All** box under the farm name. You can also select the Export job you want to import separately. Click **View Details** and you can view the

logical device that will be used for this import job and all of the jobs in the cycle. If you check a previously imported SharePoint Migration job, you can view the last imported time in the **Last Imported Time** column.

After you finish the configuration, click **Next** to go to the next step.

3. **Notification** – Send out an e-mail notification report to specified DocAve users. In the **Select a profile with address only** drop-down list, select the e-mail notification you previously configured. You can also click **New Notification Profile** to create a notification. Click **View** to view and a **User Notification Settings** window will appear. You can view the detailed setting of the notification here. Click **Edit** to edit the notification setting or click **Close** to close the window.

   After you finish the configuration, click **Next** to go to the next step.

4. **Overview** – Review your configurations. In the **Imported Plans and Settings** table, you can view the detailed information of the DocAve 6 SharePoint Migration Data import. During the setting, you can click **Back** to go to the previous step or click **Cancel** to exit the configuration GUI.
5. Click **Finish** to save the configuration and return to the Data Manger GUI or click **Cancel** to return to Data Manager GUI without saving any changes. You can open **Job Monitor** to view the job details.

Converting 3rd Party Tool Stub to DocAve Stub

If you are using a third party tool and have generated some third-party stubs, you can use this function to convert those stubs to DocAve stubs. To convert 3rd Party Tool stub to DocAve stub, go to the Control Panel, and click the **Data Manager** link under the Data Manager category in Specific Products Settings. Click the **3rd Party Tool** button on the ribbon.

Before you begin, you must configure the BLOB Provider in Storage Optimization. Click the **Blob Provider** link in the **3rd Party Tool** interface in Data Manager. For more details on how to configure Blob Provider, refer to the Configure Blob Provider section in the Storage Manager User Guide.

After you finish the configuration, return to the 3rd Party Tool GUI. Click the **Data Type** button on the ribbon and select **Import Stub**.

Complete the following steps:

1. **Prerequisites** – Have you completed the following configurations?
   - **BLOB Provider** – Ensure that you have configured the BLOB Provider in the Storage Manager prior to importing the stubs:
     - If you already configured the BLOB Provider according to the directions at the start of this section, and then select **Configured**.
     - If you have not completed this configuration, select **Not Configured** (the default selection), click the **Configure Blob Provider** link, complete your BLOB Provider configuration, return to the **Prerequisites** page, and then select **Configured**.

- **Configure Logical Device** – Ensure that you have configured a logical device to store the BLOB data of the converted third party stubs:
    - If you already configured a logical device according to the directions at the start of this section, and then select **Configured**.
    - If you have not completed this configuration, select **Not Configured** (the default selection), click the **Configure Logical Device** link, complete your logical device configuration, return to the Prerequisites page, and then select **Configured**.

Once you have selected **Configured** for both fields, click **Next** to go to the next step.

2. **Data Selection** – You are able to select where you want to convert the third-party stubs to DocAve stubs in this step.
    - **SharePoint Environment** – Browse from farm level to content database level and select the level where you want to convert the third-party stubs. Refer to the information below to select on the farm tree.
        - You can only select nodes in the same farm.
        - When selecting the farm, Web application, or content database, there will be a **Configure** button on the right. Note that this button is only for configuring the logical device for the current level you select. While the **Configure** button on the ribbon will configure the logical device for all of the selected nodes. After clicking the **Configure** button next to the node or the **Configure** button on the ribbon, select a logical device from the drop-down list or create a logical device by clicking **New Logical Device**. Click **Save** to finish the logical device configuration and go back to the Data Selection interface or click **Cancel** to exit the interface.

    After you finish the configuration, click **Next** to go to the next step.

3. **Data Settings** – Set up the configurations below:
    - **Data Compression** – This option allows you to compress BLOB data and save space. Select the **Compression** option and select a compression level. A low compression level results in a faster compression rate but a larger data set, while a high compression level results in a slower compression rate but a smaller, better quality data set. Note that small data sets occupy more system resources and cause slower job times. The compression is performed on the SharePoint Server (SharePoint Agent).
    - **Data Encryption** – If you want to enable data encryption, check **Encryption** and select security profile in the **Security Profile** drop-down list. You can also click **New Security Profile** to create a new security profile. Encryption protects sensitive materials; however, note that encrypting data causes slower extend times. The encryption is performed on the SharePoint Server (SharePoint Agent).
    - **Agent Group** – If you have several agent groups under one farm, you can select an agent group to run the stub converting job.
    - **Notification** – Select a notification profile to send out e-mail notification report to specified DocAve users. You can select previously configured notification profile in the

drop-down list or click **New Notification Profile** to create a new notification profile. For details on how to configure a notification setting, refer to the User Notification Settings section in this user guide.

- **Schedule Selection** – Set up a schedule to run the stub converting job. If you want to run the job right now, select **Start converting once finish the wizard**. If you want to set up a schedule, select **Configure the schedule myself** to have DocAve run stub converting job at a designated time. You can select the start time for the job by selecting the date from the drop-down list and entering hour and minute in the other two text boxes.

4. Click **Finish** to save the configuration and return to Data Manger GUI or click **Cancel** to return to Data Manager GUI without saving any changes. You can click **Job Monitor** on the ribbon to go to Job Monitor GUI and view the job detail.

Index Manager

Index Manager allows you to configure a full text index setting. With this function, you can search the entire content of your documents. To access Index Manager for DocAve in the Control Panel interface, click the **Index Manager** link under the Index Manager heading in Specific Products Settings.

Creating an Index Profile

To create a new index profile in Index Manager, complete the following steps:

1. Click **New Index Profile** on the ribbon.
2. Enter a Profile name in the text box. Then enter an optional **Description** for this profile for future reference.
3. Select a **Logical device** from the drop-down list to select the location to store the index data.
4. Select a **Media service** from the drop-down list, and then click **Add**. You can add multiple media services for this profile. Click **Test** to verify the connection between the media service(s) and the logical device.
5. Select one of the following options for generating a full text index:

    - **Automatically generate full text index when the job is finished** (default option) – When an Archiver job completes or completes with exception, it will trigger a full text index job. You can go to job monitor to view the job details.
    - **Generate full text index on schedule** – You can set up a schedule for the full text index job. Enter the date and time of day in the **Start time** text boxes. Enter a positive integer in the **Interval** text box for the frequency, and select either **Day(s)**, **Week(s)**, **or Month(s)** as the time unit for the interval.

    ***Note:** Your browser's time zone is selected by default. You can change the time zone by clicking on the hyperlink, and then select a new time zone from the drop-down menu and click **OK**.

6. Click **Advanced** if you want to perform a detailed configuration for any of the following fields (optional):

    - **File Type** – All the file types listed are supported for full text index search. By default, all file types are selected.

    ***Note:** If you are using the built-in PDF analyzer, only English documents can generate index. In order to better generate index for PDF documents in different languages, it is recommended to install Adobe PDF iFilter on the server where the media service for full text index is installed.

    - **File Size** – Enter an integer in the text box for size limitation of full text index. By default, the number is 100 MB. The file whose size is larger than the entered size will not be indexed. Also, generating the index for a larger file may take longer time.
    - **Preview Function** – Enable the preview of the searched content in the search result.

7. Click **Save** to save the profile and return to the Index Manager interface.

After you finish the profile configuration, go to **Storage Optimization > Archiver > Archiver Index Device** and configure the level where you want to apply full text index. For detail on how to configure Archiver Index Device, refer to the **Configuring the Archiver Index Device** section of the Archiver User Guide. The full text index will be generated according to the index profile settings and workday setting.

***Note:** If you want to change the logical device for the configured profile, a pop up window will appear asking you to copy the data from the current index device to the new one before you run the index job. Click **OK** to continue. Another pop up window will appear, asking you to save the Excel file. The file contains site information, source device information, and destination device information. Follow the instructions in the Excel file to copy the index folder from the source device to the destination device while keeping the same structure.

Configuring Workday for the Index Profile

Click the **Configuration Workday** button to globally configure the full text index setting. Running a full text index occupies space and resources on your network. The **Configure Workday** option allows you to control the full text index job based on the working hours you select.

- **Process Cap for Working Hour(s)** – Limit the maximum number of generating index jobs that can simultaneously run for each media service during work hours. By default, the maximum process number is 3. As an example, if you configured 3 media services in the index profile, you can at a maximum have 9 generating index jobs running during working hours. If you have more than 9 jobs, the job status will change to waiting for any job after the 9th.
- **Process Cap for Non-Working Hour(s)** – Limit the maximum number of generating index jobs that can simultaneously run for each media service during non-working hours. By default, the maximum process number is 3. As an example, if you configured 3 media services in the index profile, you can at a maximum have 9 generating index jobs running during non-working hours. If you have more than 9 jobs, the job status will change to waiting for any job after the 9th.

- **Define Work Hours** – Select the **Working hour(s)** by selecting times from the drop-down lists and select **Working day(s)** by selecting the checkboxes. Your browser's time zone is selected by default. If you want to change the time zone, click on the hyperlink, select a new time zone from the drop-down menu, and click **OK**. Then click **Save** on the ribbon to complete the configuration.

To edit an index profile from DocAve, select the checkbox of an index profile, and then click **Edit** on the ribbon to change the configurations for this index profile. For details on editing configurations for an index profile, see the Create an Index Profile section of this guide.

To delete an index profile from DocAve, select an index profile from the list of previously configured index profiles, and then click **Delete** on the ribbon. A confirmation window will pop up and ask if you are sure you want to proceed with the deletion. Click **OK** to delete the selected index profile(s), or click **Cancel** to return to the Index Manager interface without deleting the selected index profile(s).

Export Location

Export Location allows you to export/import data in offline Replicator jobs, import solutions in offline deployment, in offline eRoom Migration/Lotus Notes Migration/ Livelink Migration jobs, export/import data in Vault, and export/import data in Content Manager.

To access Export Location settings for DocAve in the Control Panel interface, click **Export Location** under the Export Location heading. Click **Close** on the ribbon to close the Export Location interface.

Managing Export Locations

In Export Location, you can create a new export location, view details about an export location, edit a previously configured export location, or delete a previously configured export location. For details on creating or editing an export location, refer to the Configuring Export Locations.

To view details about an export location, select it from the list of previously configured export locations, and then click **View Details** on the ribbon. You will see the previously configured settings for this export location.

Click **Edit** on the ribbon to change the configurations for this export location. For details on editing configurations for an export location, refer to the Configuring Export Locations.

To delete an export location from DocAve, select it from the list of previously configured export locations, and then click **Delete** on the ribbon. A confirmation window will pop up and ask if you are sure you want to proceed with the deletion. Click **OK** to delete the selected export location(s), or click **Cancel** to return without deleting it.

Configuring Export Locations

To create a new export location, click **Create** on the ribbon. To modify a previously configured export location, select the export location, and then click **Edit** on the ribbon. In the Create Export Location or Edit Export Location interface, configure the following settings:

1. **Name and Description** – Enter a **Name** for this export location. Then enter an optional **Description** for this export location for future reference.
2. **Farm Selection** – Select the farm where you are creating this export location. The created export location can only be used by the farm specified here.
3. **Path** – The export location can be a file share, storage area network (SAN), or network-attached storage (NAS).
    a. Enter the **UNC Path** in the following format: *admin-PC**c$**data* or *admin-PC**shared* folder.

    ***Note:** If the path you entered does not exist, it will be created automatically.

    b. Select a managed account profile from the drop-down list or click **New Managed Account Profile** to create a new one, and then click **Validation Test**. DocAve tests the path and user information to make sure they are valid.
4. Click **Save** to save the configurations and return to the Export Location interface, or click **Cancel** to return to the Export Location interface without saving any changes.

Filter Policy

Filter Policy allows you to set up filter rules so you can control what objects and data within any SharePoint level appear so that you can target content more precisely. By setting up and saving filter policies, you can apply the same filter policies to different plans without having to recreate them each time.

To access Filter Policy for DocAve in the Control Panel interface, click **Filter Policy** under the Filter Policy heading. Click **Close** on the ribbon to close the Filter Policy interface.

In the Filter Policy interface, you will see a list of previously configured filter policies.

Managing Filter Policies

In Filter Policy, you can create a new filter policy, view details about a filter policy, edit a previously configured filter policy, or delete a previously configured filter policy. For details on creating or editing a filter policy, see the Configuring Filter Policies section of this guide.

Click **Edit** on the ribbon to change the configurations for this filter policy. For details on editing configurations for filter policy, see the Configuring Filter Policies section of this guide.

To view a filter policy for DocAve, select it from the list of previously configured filter policies, and then click **View Details** on the ribbon. To delete a filter policy for DocAve, select it from the list of previously configured filter policies, and then click **Delete** on the ribbon. A confirmation window will pop up and ask if you are sure you want to proceed with the deletion. Click **OK** to delete the selected filter policy, or click **Cancel** to return without deleting it.

Configuring Filter Policies

To create a new filter policy, click **Create** on the ribbon. To modify a previously configured filter policy, select the filter policy, and then click **Edit** on the ribbon. In the Create Filter Policy or Edit Filter Policy interface, configure the following settings:

1. **Name and Description** – Enter a **Name** for the filter policy. Then enter an optional **Description** for future reference.
2. **Criteria** – Select specific objects or data within each SharePoint level (from site collection down to attachment). Each level has a unique set of rules that can be applied to enhance configurations. Refer to Appendix A: Examples of Filter Policies for examples of filter policies that users can configure.
    a. Click **Add a Filter Level Group** to add a new rule of the specified level and then click **Add a Criterion** to add criteria for the new rule by completing the fields below, and click to delete the rule that is no longer needed.
        - **Rule** – Select the new rule you want to create from the drop-down list.

          ***Note:** The site level filter policy using the **Created By** rule cannot be used for SharePoint Online environment.
        - **Condition** – Select the condition for the rule.
        - **Value** – Enter a value you want the rule to use in the text box.

    b. To add more filters to the filter policy, repeat the previous step.

       ***Note:** Depending on the filters you enter, you can change the logical relationships between the filter rules. There are currently two logical relationships: **And** and **Or**. By default, the logic is set to **And**. To change the logical relationship, click on the logical relationship link. The **And** logical relationship means that the content which meets all of the rules will be filtered and included in the result. The **Or** logic means that the content which meets any one of the rules will be filtered and included in the result. The **Or** logical relationship only applies to the same level of rules.
3. **Basic Filter Condition** – View the logical relationship of the filter rules in this area.

   For example, if the logical relationship is ((1 Or 2) And 3) in the Basic Filter Condition area, the contents that meet the filter rule 3 either meets the filter rule 1 or filter rule 2 will be filtered and included in the result.

Click **Save** to save the configurations and return to the Filter Policy interface, or click **Cancel** to return to the Filter Policy interface without saving any changes.

***Note:** Run an Audit Controller Retrieve Data job before you implement the Last Accessed Time rule on the selected node. For more information about how to run an Audit Controller Retrieve Data job, please refer to the Archiver User Guide.

Host Profile

Use **Host Profile** to store the necessary information so that you can connect to the host successfully. Host Profile can be used in the Platform Backup & Restore and VM Backup & Restore modules.

To access **Host Profile**, click **Host Profile** under the **Host Profile Manager** heading.

In the **Host Profile Manager** interface, you will see a list of host profiles.

You can create, view details, edit, or delete a host profile. For more information, refer to Creating a Host Profile, Viewing Details about a Host Profile, Editing a Host Profile, and Deleting Host Profiles respectively.

Creating a Host Profile

To create a new host profile, click **Create** on the ribbon. In the **Create** interface, you can configure the following settings:

1. **Host Profile Name** – Enter a **Name** for this host profile. Then, enter an optional **Description** for future reference.
2. **VM Host Type** – Select a **VM Host Type** from the drop-down list.
    - **ESX/ESXi** – Select this option if you want to connect to an **ESX/ESXi** host.
    - **Hyper-V** – Select this option if you want to connect to a **Hyper-V** host.
    - **vCenter –** Select this option if you want to connect to a **vCenter** host.
3. **Agent** – Select an **Agent** to validate if it can connect to the host successfully.

    ***Note:** In terms of Hyper-V, the Agent must be installed on the host server. There is only one host profile that you can create for each Hyper-V host server.

    ***Note:** In terms of ESX/ESXi and vCenter, there is no need for the Agent to be installed on the host server and you can create more than one host profile for each ESX/ESXi or vCenter host server.

    ***Note:** In terms of Hyper-V, if the Agent you selected has been used to create a Hyper-V host profile, when you try to save the configurations, a window will pop up to inform you that you cannot select this Agent because it is currently being used by another Hyper-V host profile.

***Note:** A Hyper-V host profile only supports the following operating systems for the host server where the selected Agent is installed: Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2012, and Microsoft Hyper-V Server 2012 R2.

4. **IP Address/Hostname** – Enter the **IP Address/Hostname** of the host you are about to connect.

   ***Note:** If you select **Hyper-V** as the **VM Host Type**, then you cannot change the value in the **IP Address/Hostname** field.

5. **Credentials** – Enter the **Username** and **Password** to connect to the specified host server if you select **ESX/ESXi** or **vCenter** as the **VM Host Type**. It is recommended that the user whose name is entered here have the administrator role to the host server.

   ***Note:** If the user does not have the administrator role to the host server, ensure that this user is assigned the minimum privileges listed in Required Minimum Privileges for ESX/ESXi or vCenter Host Profile table.

6. **Managed Account Profile** – Displays the Agent account of the selected Agent. If you select **Hyper-V** as the **VM Host Type**, this field will appear in place of **Credentials**. You cannot change the value in this field, either.
7. Click **Validation Test** to verify that the information you entered is correct.
8. Click **Save** on the ribbon or the **Save** button on the lower-right corner of the wizard to save your configurations and return to the **Host Profile Manager** interface. Click **Cancel** on the ribbon or the **Cancel** button on the lower-right of the wizard to return to the **Host Profile Manager** interface without saving any changes.

Required Minimum Privileges for ESX/ESXi or vCenter Host Profile

If the user does not have the administrator role to the host server, ensure that this user's permissions meet the minimum privileges listed in the table below:

Privileges		
Datastore	Allocate space	
	Browse datastore	
	Low level file operations	
	Remove file	
Folder	Create folder	
Resource	Assign vApp to resource pool	
	Assign virtual machine to resource pool	
	Create resource pool	
vApp	Add virtual machine	
	Assign resource pool	
	Assign vApp	
	Create	
Network	Assign network	
Virtual machine	Configuration	
	Interaction	Answer question

Privileges		
		Configure CD media
		Configure floppy media
		Device connection
		Power On
		Power Off
	Inventory	Create new
		Register
		Remove
		Unregister
	Snapshot management	Create snapshot
		Remove Snapshot
	Provisioning	Allow disk access
		Allow read-only disk access
Permission	Modify permissions	
	Modify role	
Global	DisableMethods	
	EnableMethods	
	License	

Viewing Details about a Host Profile

Select a host profile by selecting the corresponding checkbox, and then click **View Details** on the ribbon or click on the name of the desired host profile to view the detailed information of the selected host profile.

Editing a Host Profile

To edit a host profile, select the host profile by selecting the corresponding checkbox, and then click **Edit** on the ribbon, or you can click on the name of the desired host profile to go to the **View Details** interface first and then click **Edit** on the ribbon. The **Edit** interface appears.

All of the configurations in the **Edit** interface are the same as those in the **Create** interface, so for more information about how to configure these values, refer to Creating a Host Profile.

Click **Save** on the ribbon or the **Save** button on the lower-right corner of the wizard. A confirmation window will pop up and ask if you are sure to save your configurations because the profile you are about to edit maybe is currently being used by one or more plans/profiles, and any changes made to it will affect all of these plans/profiles. Or you can click **Cancel** on the ribbon or the **Cancel** button on the lower-right of the wizard to return to the **Host Profile Manager** interface without saving any changes.

Deleting Host Profiles

To delete host profiles, select the host profiles from the list of previously configured host profiles, and click **Delete** on the ribbon. Click **OK** to confirm the deletion.

After finishing viewing and managing your host profiles, click **Cancel** on the ribbon to exit the **Host Profile Manager** interface and go back to the **Control Panel** interface.

Mapping Manager

Mapping Manager allows you to map properties of the source node to the properties of the destination node. There are eight types of mappings you can create in Mapping Manager:

- **Domain Mapping** – Maps a source domain to a destination domain. The destination domain name will be replaced by the configured source domain name, and the user in the source group will be mapped to the destination user of the same name. By creating a rule for domain mapping, any plans using the rule can repeat the process without having to manually re-enter the settings.

  ***Note:** It is not supported to use Domain Mapping to map the source AD group to the destination SharePoint Online farm. Use Group Mapping instead to map the AD group to the destination SharePoint Online farm.

  For example, organization A has a subsidiary B. Organization B's employees all have their domain accounts in organization A's domain and vice versa. When you want to replicate A's sites to the internal sites of B, you can use domain mapping to bulk map these users to their accounts in B's domain. In other words, you can use domain mapping to bulk change the users' domain when two domains have the same user accounts.

- **User Mapping** – Maps a source user to a target user. This way, if the same user has a different username in Domain A than in Domain B, or if you want to migrate an individual user's content, permissions, and metadata in Domain A to another user in Domain B, the user's permissions and metadata will not be lost when content is moved.

  For example, organization A takes over organization B; however, the two companies have their own domains. If you want to replicate organization B's employee site to the internal site of organization A, you can use user mapping to map this user's account in B's domain to A's domain. In other words, user mapping can map the user's account in two different domains, so the permissions and metadata in SharePoint will not be lost after moving one user's SharePoint content to another domain.

- **Language Mapping** – Displays the source content in a different language than the destination node.

  For example, organization A has a subsidiary B in a different country. When replicating A's sites to B's SharePoint farm, you can use language mapping to make sure all of the list and column names are displayed in B's language. In other words, you can use language mapping to change the display language after replicating the source content to another SharePoint farm in a different country.

- **Column Mapping** (used by Content Manager, SharePoint 2007 to 2013 Migration, SharePoint 2010 to 2013 Migration, and SharePoint 2007 to 2010 Migration) – Maps a source column to a target column. The destination column name will be replaced by the configured source column name, and you are able to add value mapping. By creating a condition on different levels, you can create the rule you want.

  For example, column A is on the source side and column B is on the destination side. If you want to replicate column A to column B, you can use column mapping to map this column's metadata to the destination.

- **Content Type Mapping** (only used by Content Manager, and Migration) – Maps a source content type to a target content type. The source content type will be replaced by the configured destination content type.

  For example, content type A is on the source side and content type B is on the destination side. If you want to replicate content type A to content type B, you can use content type mapping to map this content type to the destination.

- **Template Mapping** (only used by Content Manager, and Migration) – Maps a source template to a target template. The destination content type will be replaced by the configured destination template. You will be able to create mapping at the site level and list level.

  For example, template A is on the source side and template B is on the destination side. If you want to replicate template A to template B, you can use template mapping to map this template to the destination.

- **Group Mapping** (only used by non-SharePoint Migration) – Maps a source group to a target group. The source group will be replaced by the configured group.

  For example, group A is on the source side and group B is on the destination side. If you want to replicate group A to group B, you can use group mapping to map this group to the destination.

- **List Name Mapping** – Maps a source list name to a destination list name. The source list name will be replaced by the configured list name.

  For example, list A is on the source side and list B is on the destination side. If you want to replicate list A to list B, you can use list name mapping to map this list to the destination.

Domain Mapping

To access **Domain Mapping** for DocAve, click **Domain Mapping** under the **Mapping Manager** heading in the **Control Panel** interface. You will be brought to the **Domain Mapping** interface. Click **Close** on the ribbon to close **Mapping Manager**.

In the Domain Mapping configuration interface, you will see a list of previously configured domain mappings.

Managing Domain Mappings

In the **Domain Mapping** interface, you can create a new domain mapping, view details about a domain mapping, edit a previously configured domain mapping, delete a previously configured domain mapping, or export a domain mapping. For details on creating or editing a domain mapping, see the Configuring Domain Mappings section of this guide.

To see the configurations of a domain mapping, select it from the list of previously configured domain mappings, and then click **View** on the ribbon. The configuration details will appear. Click **Export** on the ribbon to export this domain mapping, or click **Edit** to change the configurations.

To change the configurations of a domain mapping, select it from the list of previously configured domain mappings, and then click **Edit** on the ribbon. For details on editing configurations for a domain mapping, see the Configuring Domain Mappings section of this guide.

To export a domain mapping to an XML file, select it from the list of previously configured domain mappings, and then click **Export** on the ribbon. Exported domain mappings can be imported when creating or editing a domain mapping to expedite the process.

Configuring Domain Mappings

To create a new domain mapping, click **Create** on the ribbon. To modify a previously configured domain mapping, select the checkbox next to the domain mapping, and then click **Edit** on the ribbon. In the Create Domain Mapping or Edit Domain Mapping interface, complete the following steps:

1. Configure the following settings for the domain mapping:
    - **Name and Description** – Enter the **Name** as you want it to appear for the new domain mapping profile. Enter an optional **Description** for this domain mapping profile for future reference.
    - **Add Mapping Rules** – Enter the **Source Domain Name** and the **Destination Domain Name**. The specified source domain name will be replaced by the specified destination domain name after the corresponding job completes.
2. Click **Add**. The new rule appears in the **Source Domain Name** and **Destination Domain Name** display table.

    To delete a mapping rule, select the checkbox next to the mapping rule(s) you want to delete, and then click **Delete**.

3. Click **Save** to save the configurations for this domain mapping and return to the Domain Mapping interface in Mapping Manager, or click **Cancel** to return without saving any of your changes.

User Mapping

To access User Mapping for DocAve in the **Control Panel** interface, click **User Mapping** under the **Mapping Manager** heading. You will be brought to the **User Mapping** interface. Click **Close** on the ribbon to close **Mapping Manager**.

In the User Mapping configuration interface, you will see a list of previously configured user mappings.

Managing User Mappings

In the **User Mapping** interface, you can create a new user mapping, view details about a previously configured user mapping, edit a previously configured user mapping, delete a previously configured user mapping, or export a user mapping. For details on creating or editing a user mapping, see the Configuring User Mappings section of this guide.

To see the configurations of a user mapping, select it from the list of previously configured user mappings, and then click **View** on the ribbon. The configuration details will appear. Click **Export** on the ribbon to export this user mapping, or click **Edit** to change the configurations.

To change the configurations of a user mapping, select it from the list of previously configured user mappings, and then click **Edit** on the ribbon. For details on editing configurations for a user mapping, see the Configuring User Mappings section of this guide.

To export a user mapping to an XML file, select it from the list of previously configured user mappings, and then click **Export** on the ribbon. Exported user mappings can be imported when creating or editing a user mapping to expedite the process.

Configuring User Mappings

To create a new user mapping, click **Create** on the ribbon. To modify a previously configured user mapping, select the user mapping, and then click **Edit** on the ribbon. In the **Create User Mapping** or **Edit User Mapping** interface, complete the following steps:

1. Configure the following settings for the user mapping:
    - **Name and Description** – Enter the **Name** as you want it to appear for the new user mapping profile. Enter an optional **Description** for this user mapping profile for future reference.
    - **Add Mapping Rules** – Configure the user mapping by entering the Source Username and Destination Username into the provided field. The specified Source Username will be replaced by the specified Destination Username after the corresponding job completes. Enter the username in Source default user, Target default user and Destination Username according to the displayed formats.

      ***Note:** The mapping rules examples of each kind of users or groups are provided as:

- **Classic Windows User & Group** – Domain (NETBIOS)\username (e.g. domain\user)
- **FBA User & Role** – Provider: username (e.g. ldapMembershipProvider:user, sqlRoleProvider:role)
- **SharePoint Online User** – (e.g. membership:pm@domainbeta.onmicrosoft.com, i:0#.f|membership|pm@domainbeta.onmicrosoft.com)
- **Claim (Exclude FBA) User & Role** – full login name (e.g. i:0#.w|domain\user, c:0!.s|window, c:0+.w|s-1-5-27-0123456789-0123456789-0123456789-0123, i:05.t|adfs|user@domain.com, c:05.t|adfs|role)

2. Click **Add**. The new rule appears in the **Source Username** and **Destination Username** display table.

   To delete a mapping rule, select the mapping rule(s) you want to delete by selecting the checkbox. Click **Delete**.

3. Click **Save** to save the configurations for this user mapping, and return to the User Mapping interface in Mapping Manager, or click **Cancel** to return to without saving any of your changes.

User Mapping Discrepancy Resolutions

There are situations where the **Source Username** cannot be mapped to the **Destination Username**. In the **Add Mapping Rules** section, you may choose to use the default resolution, or customize the settings for resolving such discrepancies.

***Note**: The **Source default user** and **Source place holder** for the source node are only used in two-way replication.

To have the non-existent destination user replaced by the DocAve agent account, deselect the checkbox next to **Customize settings if the user does not exist in destination**.

To have the non-existent destination user replaced by a user of your choice, select the **Customize settings if the user does not exist in the destination** checkbox, select **Add a default destination user**, and enter a default destination user in the **Target Default User** text box.

To have the non-existent destination user replaced by the corresponding source users, add a place holder account in the destination **Active Directory**, and then perform the following operations:

1. Select the **Customize settings if the user does not exist in the destination** checkbox.
2. Select **Add a place holder account to keep metadata even if the user no longer exists** (Not supported for SharePoint Online environments.)
3. Enter the placeholder account that you added in the Active Directory in the **Target placeholder** text box.

***Note**: If the Default User and the Placeholder Account have been added in the Active Directory of the destination, you can set up the user mapping profile in DocAve directly. If not, before setting up the user

mapping profile in DocAve, you must manually add the Target Default User and the Target Placeholder Account in the Active Directory of the destination. For security reasons, it is recommended that you enter a user who exists in the destination Active Directory but does not exist as the placeholder account in SharePoint to avoid unintentionally giving a SharePoint user access to any data assigned to the placeholder account.

***Note**: Receiving notification that **The user does not exist in destination** means one of the following scenarios is true:

- The destination user's account is no longer active/valid.
- The source user and the destination user are in different domains, and there is no domain mapping or user mapping for these two domains.
- The source user and the destination user are in different domains, and the specified user cannot be mapped using any of the configured domain mapping or user mapping.
- The source user and the destination user are in different domains, and there is a domain mapping for these two domains, but there is no destination user with the same name as the source user.

Language Mapping

To access Language Mapping for DocAve in the Control Panel interface, click **Language Mapping** under the Mapping Manager heading. You will be brought to the Language Mapping interface. Click **Close** on the ribbon to close Mapping Manager.

In the Language Mapping configuration interface, you will see a list of previously configured language mappings.

Managing Language Mappings

In the **Language Mapping** interface, you can create a new language mapping, view details about a previously configured language mapping, edit a previously configured language mapping, delete a previously configured language mapping, or export a language mapping. For details on creating or editing a language mapping, see the Configuring Language Mappings section of this guide.

To see the configurations of a language mapping, select it from the list of previously configured language mappings, and then click **View** on the ribbon. The configuration details will appear. Click **Export** on the ribbon to export this language mapping, or click **Edit** to change the configurations.

To change the configurations of a language mapping, select it from the list of previously configured language mappings, and then click **Edit** on the ribbon. For details on editing configurations for a language mapping, see the Configuring Language Mappings section of this guide.

To export a language mapping to an XML file, select it from the list of previously configured language mappings, and then click **Export** on the ribbon. Exported language mappings can be imported when creating or editing a language mapping to expedite the process.

Configuring Language Mapping

To create a new language mapping, click **Create** on the ribbon. To modify a previously configured language mapping, select the language mapping, and then click **Edit** on the ribbon. In the Create Language Mapping or Edit Language Mapping interface, complete the following steps:

1. Configure the following settings for the language mapping:
    a. **Name and Description** – Enter the **Name** as you want it to appear for the new language mapping profile. Enter an optional **Description** for this language mapping profile for future reference.
    b. **Source language** and **Target language** – Select the language from the drop-down menu that the source node is displayed in and the language that you want to have the destination node display. After running a plan with this Language Mapping Rule, the destination node will be displayed in the **Target language** field.

       ***Note**: The following languages are available for mapping: English, Japanese, and German.

    c. **Add Mapping Rules** – Select **List** or **Column** from the drop-down menu. Enter the name of the list or column used in the source language in the text box. Enter the name of the list or column you want the target language to use in the destination node. The source column or list name will be replaced by the specified destination column or list name.
2. Click **Add**. The new rule appears in the **Type**, **Source Language**, and **Target Language** display table.

   To delete a mapping rule, select the checkbox next to the mapping rule(s) you want to delete. Click **Delete**.

3. Click **Save** to save the configurations for this language mapping, and return to the Language Mapping interface in Mapping Manager, or click **Cancel** to return without saving any of your changes.

Column Mapping

To access Column Mapping for DocAve in the Control Panel interface, click **Column Mapping** under the Mapping Manager heading. You will be brought to the Column Mapping interface. Click **Close** on the ribbon to close Mapping Manager.

In the Column Mapping configuration interface, you will see a list of previously configured column mappings.

Managing Column Mappings

In the **Column Mapping** interface, you can create a new column mapping, view details about a previously configured column mapping, edit a previously configured column mapping, delete a previously configured column mapping, or export a column mapping. For details on creating or editing a column mapping, see the Configuring Column Mappings section of this guide.

To see the configurations of a column mapping, select it from the list of previously configured column mappings, and then click **View** on the ribbon. The configuration details will appear. Click **Export** on the ribbon to export this column mapping, or click **Edit** to change the configurations.

To change the configurations for this column mapping, select it from the list of previously configured column mappings, and then click **Edit** on the ribbon. For details on editing configurations for a column mapping, see the Configuring Column Mappings section of this guide.

To export a column mapping to an XML file, select it from the list of previously configured column mappings, and then click **Export** on the ribbon. Exported column mappings can be imported when creating or editing a column mapping to expedite the process.

Configuring Column Mapping

To create a new column mapping, click **Create** on the ribbon. To modify a previously configured column mapping, select the column mapping, and then click **Edit** on the ribbon. In the Create Column Mapping or Edit Column Mapping interface, complete the following steps:

1. Configure the following settings for the column mapping:
    a. **Name and Description** – Enter the **Name** as you want it to appear for the new column mapping profile. Enter an optional **Description** for this column mapping profile for future reference.
    b. **Condition** – Filters the condition for site, list, and item level.
        - In the site level, click **Add a Condition**. In the first drop-down list, you can select **URL** or **Site Content Type** as a rule. In the second drop-down list, you can select **Equals**, **Does Not Equal**, **Contains**, or **Does Not Contain** as the condition. In the third text box, you can enter the value you want to filter. If you want to configure another site condition, click the add ( ) button to add a new site condition configuration tab. Click the show details ( ) button to select the site condition you previously configured.
        - In the list level, click **Add a Condition**. In the first drop-down list, you can select **Template ID**, **List Title**, or **List Content Type** as a rule. In the second drop-down list, you can select **Equals**, **Does Not Equal**, **Contains**, or **Does Not Contain** as condition. If you select **Template ID** as a rule, you can view commonly used templates. If you cannot find all of the templates you want, select **Customized** at the bottom of the drop-down list and enter the template name you want in the text box on the right. If you select **List Title** or **List Content Type** as a rule,

you can enter the value you want to filter in the text box. If you want to configure another list condition, click the add ( ) button to add a new list condition configuration tab. Click the show details ( ) button to select the List condition you previously configured.

***Note:** The source list and destination list must have the same name.

- In the item level, click **Add a Condition**. You can select **Document Name** in the first drop-down list. In the second drop-down list, you can select **Equals**, **Does Not Equal**, **Contains**, or **Does Not Contain** as condition. In the third text box, you can enter the value you want to filter. If you want to configure another site condition, click the add ( ) button to add a new item condition configuration tab. Click to select the item condition you previously configured.

  ***Note**: Regarding relation between different conditions, refer to the tips below:

  - If you keep null for the text boxes in all levels, column mappings will be deployed into site columns and list columns.
  - If you only enter condition on site level, the site column and list column meet this condition will deploy the mapping.
  - If you only enter condition for list and item level, the list column meet this condition will use the mapping.
  - If a site column and list column meet conditions for multiple mappings, the first mapping will be deployed.

  ***Note**: Regarding the relation between different mappings and levels, refer to the tips below:

  - The relation between different mappings is **OR**. If an object meets the condition of the first mapping, it will not compare with the second mapping.
  - The relation between different levels is **AND**. The relation between the same level is **OR** (for example, between list 1 and list 2 is **OR**).
  - On the same level and same tab, the relation between conditions is **AND** by default, you can click **AND** and it will change to **OR**.

c. **Column Mapping** – Configure more column mapping settings by completing the following steps:

- Click the show details ( ) button in the **Column Type** field. In the drop-down list, select Same Type, Change to Destination, Change to Managed Metadata, or Change to Lookup.
  - If you select **Same Type**, the source and destination column type must be the same, or you cannot use mapping. If the column types are the same on source and destination, the column type on the source will be mapped to the destination. If the column types is different on source and destination, DocAve will create a new columns on the destination.

- If you select **Change to Destination**, it represents that the column type can be different on source to destination.

  ***Note:** If the column already exists on destination, the source column type will be mapped to the destination. If the column type does not exist in the destination, DocAve will create a new column in the destination.

- If you select **Change to Managed Metadata**, the column type mapping to the destination is Managed Metadata.

  ***Note:** If the column existing on the destination is a Managed Metadata column, the source column type will be mapped to the destination. If the column existing in the destination is not a Managed Metadata column, DocAve will create a new a Managed Metadata column in the destination with the same name as the source column. If the column does not exist on the destination, DocAve will create a new Managed Metadata column.

  To separate character strings into different columns, click **Settings** to configure **Allow multiple term values** and **Migrate string separated with ; into columns**. These two options are selected by default. You can enter any character into the ; text box to separate the columns. In **Term set path**, you can enter the term path to locate the term. The character string you enter must have an acceptable format, for example **Term Group**; **Term Set**; **Term**.

- If you select **Change to Lookup**, it represents that you want to map the source column to the lookup column in destination. If the Lookup Column does not exist on the destination, DocAve will create a new lookup column according to your settings on the destination.

  To separate character strings into different columns, click **Settings** to configure **Allow multiple term values** and **Migrate string separated with ; into columns**. In the **List title** text box, you can enter the list title. In the **Column name** text box, you can enter the column name.

- In the **Column Mapping** table, you can enter the **Column Name** and **Internal Name** for source and destination. The column name is the display name. If you enter both the column name and the internal name, DocAve will recognize the internal name first. You must enter at least one group of source/destination in order to add a value mapping or save the profile. Click **Add a Value Mapping** and enter the column value you want to map from the source to destination.

***Note**: If you enter a value in the source side but keep it null in the destination side, this column will not be migrated to the destination. If you keep it empty in source side and enter a value in

destination, DocAve will migrate the empty value of the source to the value you configured in the destination.

2. Click **Save** to save the configurations for this column mapping, and return to the Column Mapping interface in Mapping Manager, or click **Cancel** to return without saving any of your changes.

Content Type Mapping

To access Content Type Mapping for DocAve in the **Control Panel** interface, click **Content Type Mapping** under the Mapping Manager heading. You will be brought to the Content Type Mapping interface. Click **Close** on the ribbon to close Mapping Manager.

In the Content Type Mapping configuration interface, you will see a list of previously configured content type mappings.

Managing Content Type Mappings

In the Content Type Mapping interface, you can create a new content type mapping, view details about a previously configured content type mapping, edit a previously configured content type mapping, delete a previously configured content type mapping, or export a content type mapping.

To see the configurations of a content type mapping, select it from the list of previously configured content type mappings, and then click **View** on the ribbon. The configuration details will appear. Click **Export** on the ribbon to export this content type mapping, or click **Edit** to change the configurations.

To change the configurations for this content type mapping, select it from the list of previously configured content type mappings, and then click **Edit** on the ribbon. For details on editing configurations for a content type mapping, see the Configuring Content Type Mapping section of this guide.

To export a content type mapping to an XML file, select it from the list of previously configured content type mappings, and click **Export** on the ribbon. Exported content type mappings can be imported when creating or editing a content type mapping to expedite the process.

Configuring Content Type Mappings

To create a new content type mapping, click **Create** on the ribbon. To modify a previously configured content type mapping, select the content type mapping, and then click **Edit** on the ribbon. In the Create Content Type Mapping or Edit Content Type Mapping interface, complete the following steps:

1. Configure the following settings for the column mapping:
    a. **Name and Description** – Enter the name as you want it to appear for the new column mapping profile. Enter an optional description for this column mapping profile for future reference.

b. **Condition** – Filter the condition for site and list level.

   - In the site level, click **Add a Condition** to add a new condition. In the first drop-down list, you can select **URL** as rule. In the second drop-down list, you can select **Equals**, **Does Not Equal**, **Contains**, or **Does Not Contain** as a condition. In the third text box, you can enter the value you want to filter. If you want to configure another site condition, click + to add a new site condition configuration tab. Click ▾ to select the site condition you previously configured.
   - In List level, click **Add a Condition** to add a new condition. In the first drop-down list, you can select **Template ID** and **List Title** as rule. In the second drop-down list, you can select **Equals**, **Does Not Equal**, **Contains**, or **Does Not Contain** as a condition. If you select **Template ID** as a rule, you can view all templates you have deployed and select the templates you want as a condition. If you select **List Title** as a rule, you can enter the value you want to filter in the text box. If you want to configure another list condition, click + to add a new list condition configuration tab. Click ▾ to select the list condition you previously configured.

c. **Content Type Mapping** – In the content type mapping table, you can enter content type names in the source and destination. Click **Add a Content Type Mapping** to add a new mapping.

2. Click **Save** to save the configurations for this content type mapping, and return to the Content Type Mapping interface in Mapping Manager.

Template Mapping

To access Template Mapping for DocAve in the Control Panel interface, click **Template Mapping** under the Mapping Manager heading. You will be brought to the Template Mapping interface. Click **Close** on the ribbon to close Mapping Manager.

In the Template Mapping configuration interface, you will see a list of previously configured template mappings.

Managing Template Mappings

In the Template Mapping interface, you can create a new template mapping, view details about a previously configured template mapping, edit a previously configured template mapping, delete a previously configured template mapping, or export a template mapping.

To see the configurations of a template mapping, select it from the list of previously configured template mappings, and then click **View** on the ribbon. The configuration details will appear. Click **Export** on the ribbon to export this template mapping, or click **Edit** to change the configurations.

To change the configurations for this template mapping, select it from the list of previously configured template mappings, and then click **Edit** on the ribbon. For details on editing configurations for a template mapping, see the Configuring Template Mapping section of this guide.

To export a template mapping to an XML file, select it from the list of previously configured template mappings, and click **Export** on the ribbon. Exported template mappings can be imported when creating or editing a template mapping to expedite the process.

Configuring Template Mappings

To create a new template mapping, click **Create** on the ribbon. To modify a previously configured template mapping, select the template mapping, and then click **Edit** on the ribbon. In the Create Template Mapping or Edit Template Mapping interface, complete the following steps:

1. Configure the following settings for the template mapping:
    a. **Name and Description** – Enter the name as you want it to appear for the new column mapping profile. Enter an optional description for this template mapping profile for future reference.
    b. **Mappings** – Set up template mappings on site or list level.
        - On the Site Template Mapping tab, click **Add a Site Template Mapping**. In the table, you can enter a template ID into the **Source** text box or select a template ID from the drop-down list. To add another site template mapping, click **Add a Site Template Mapping**. You must enter at least one mapping into the template mapping table.
        - On the List Template Mapping tab, click **Add a List Template Mapping**. In the table, you can enter a template ID into the text box or select a template ID from the drop-down list. To add another site template mapping, click **Add a List Template Mapping**. You must enter at least one mapping into the template mapping table.
2. Click **Save** to save the configurations for this template mapping, and return to the Template Mapping interface in Mapping Manager, or click **Cancel** to return without saving any changes made.

Group Mapping

To access Group Mapping for DocAve in the Control Panel interface, click **Group Mapping** under the Mapping Manager heading. You will be brought to the Group Mapping interface. Click **Close** on the ribbon to close Mapping Manager.

In the Group Mapping configuration interface, you will see a list of previously configured group mappings.

Managing Group Mappings

In the Group Mapping interface, you can create a new group mapping, view details about a previously configured group mapping, edit a previously configured group mapping, delete a previously configured group mapping, or export a group mapping. For details on creating or editing a group mapping, see the Configuring Group Mappings section of this guide.

To see the configurations of a group mapping, select it from the list of previously configured group mapping, and then click **View** on the ribbon. The configuration details will appear. You can click **Export** on the ribbon to export this group mapping, or click **Edit** to change the configurations.

To change the configurations of a group mapping, select it from the list of previously configured group mappings, click **Edit** on the ribbon. For details on editing configurations for a group mapping, see the Configuring Group Mappings section of this guide.

To export a group mapping to an XML file, select it from the list of previously configured group mappings, and click **Export** on the ribbon. Exported group mappings can be imported when creating or editing a group mapping to expedite the process.

Configuring Group Mappings

To create a new group mapping, click **Create** on the ribbon. To modify a previously configured group mapping, select the group mapping, and then click **Edit** on the ribbon. In the Create Group Mapping or Edit Group Mapping interface, complete the following steps:

1. Configure the following settings for the Group Mapping:
    a. **Name and Description** – Enter the name as you want it to appear for the new group mapping profile. Enter an optional description for this group mapping profile for future references.
    b. **Add Mapping Rules** – Maps the source group with destination group. Enter the **Source Group Name** and **Destination Group Name** into the table. Click to delete a previously configured group mapping. You can also select the checkbox next to Source Group Name, and then click **Delete Selected Mapping(s)**. You can also click **Add a Group Mapping** to add a Group.
2. Click **Save** to save the configurations for this group mapping, and return to the Group Mapping interface in Mapping Manager, or click **Cancel** to return without saving any of your changes.

List Name Mapping

To access List Name Mapping for DocAve in the Control Panel interface, click **List Name Mapping** under the Mapping Manager heading. You will be brought to the **List Name Mapping** interface.

In the List Name Mapping configuration interface, you will see a list of previously configured list name mappings.

Managing List Name Mappings

In the List Name Mapping interface, you can create a new list name mapping, view details about a previously configured list name mapping, edit a previously configured list name mapping, delete a previously configured list name mapping, or export a list name mapping. For details on creating or editing a list name mapping, refer to Configuring List Name Mappings.

To see the configurations of a list name mapping, select it from the list of previously configured list name mapping, and then click **View** on the ribbon. The configuration details will appear. You can click **Export** on the ribbon to export this list name mapping, or click **Edit** to change the configurations.

To change the configurations of a list name mapping, select it from the list of previously configured list name mappings, click **Edit** on the ribbon. For details on editing configurations for a list name mapping, refer to Configuring List Name Mappings.

To export a list name mapping to an XML file, select it from the list of previously configured list name mappings, and click **Export** on the ribbon. Exported list name mappings can be imported when creating or editing a list name mapping to expedite the process.

Configuring List Name Mappings

To create a new list name mapping, click **Create** on the ribbon. To modify a previously configured list name mapping, select the list name mapping, and then click **Edit** on the ribbon. In the Create List Name Mapping or Edit List Name Mapping interface, complete the following steps:

1. Configure the following settings for the List Name Mappings:
    a. **Name and Description** – Enter the name as you want it to appear for the new list name mapping profile. Enter an optional description for this list name mapping profile for future reference.
    b. **Condition** – Filters the condition for site and list level.
        - In the site level, click **Add a Condition**. In the first drop-down list, you can select **URL** as a rule. In the second drop-down list, you can select **Equals**, **Does Not Equal**, **Contains**, or **Does Not Contain** as the condition. In the third text box, you can enter the value you want to filter. If you want to configure another site condition, click **Add a Condition** to add a new site condition configuration tab.
        - In the list level, click **Add a Condition**. In the first drop-down list, you can select **Template ID** as a rule. In the second drop-down list, you can select **Equals**, **Does Not Equal**, **Contains**, or **Does Not Contain** as condition. You can view commonly used templates in the third text box. If you cannot find all of the templates you want, select **Customized** at the bottom of the drop-down list and enter the template name you want in the text box on the right. Click **Add a Condition** to add a new list condition configuration tab.

    On the same level and same tab, the relation between conditions is **AND** by default. You can click **AND** and it will change to **OR**.

c. **List Name Mapping** – Maps the source list name with destination list name. Enter the **Source List Name** and **Destination List Name** into the table. Click to delete a previously configured list name mapping. You can also click **Add a List Name Mapping** to add a new list name mapping.

2. Click **Save** to save the configurations for this list name mapping, and return to the List Name Mapping interface in Mapping Manager, or click **Cancel** to return without saving any of your changes.

Click **Close** on the ribbon to close Mapping Manager.

Plan Group

Plan Group provides an interface to collect plans and form them into groups according to your setup. The plans will run simultaneously or in sequence instead of you running the plans manually. In the DocAve GUI, Plan Group is located next to Job Monitor on the home screen. Click the plan group ( ) button to enter the Plan Group GUI.

***Note**: A plan group contains plans from multiple DocAve products. Only when you have valid licenses for the corresponding products can you use the plan group functions normally. In the Plan Group configuration interface, you will see a list of previously configured plan groups.

Security Trimming for Plan Group

Plan Group also follows the security trimming rule of DocAve 6. For instructions on how to configure permission levels, refer to Security Trimming Users.

Regarding permission control for Plan Group, if the specified user does not have permission to a product, this user will not be able to view or select the specific product in the **Module** drop-down list from the **Add Plan(s)** interface. If the user previously had permission to a specified product and he/she created a plan group including the plans of the specified product, and then he/she can still view the settings of the previously created plan group after the permission to this product has been removed. However, the user cannot modify the settings of the plans for the specified product (where he/she does not have permission) anymore.

Managing Plan Group

In the **Plan Group** interface, you can create a new plan group, view details about a plan group, edit a previously configured plan group, or delete a previously configured plan group. For details on creating a plan group, refer to Creating a Plan Group.

To view details about a plan group, select it from the list of previously configured plan groups, and click **View Details** on the ribbon. The previously configured settings for this plan group will appear. You can view all of the plans you have added to the plan group in the **Plan Viewer** and view the settings of the plan group itself in the **Group Settings** view.

Click **Edit** on the ribbon to change the configurations for this plan group. For details on editing configurations for a plan group, refer to Creating a Plan Group.

To delete a plan group from DocAve, select it from the list of previously configured plan groups, and click **Delete** on the ribbon. A confirmation window will pop up and ask if you are sure you want to proceed with the deletion. Click **OK** to delete the selected plan groups, or click **Cancel** to return to the **Plan Group** interface without deleting the selected plan groups.

***Note:** You cannot delete a plan group that is currently running.

To run the plans in the specified plan group, select the plan group and click **Run Now** on the ribbon. Then you will be able to view the corresponding jobs in the **Job Monitor** interface by clicking the **Job Monitor** link or clicking **Job Monitor** on the ribbon.

Creating a Plan Group

In the Plan Group interface, click Create on the ribbon. The plan group creation wizard appears.

To create a new plan group, complete the following steps:

***Note**: Even if you currently have no plans configured in DocAve, you can still create an empty plan group containing no plans and save it for future use.

1. **Plan Group Name** – Enter a group name in the **Plan group name** text box and enter an optional description in the **Description** text box for future reference.
2. Click **Next** on the ribbon or the **Next** button on the lower-left corner of the wizard to go to the next step.

   ***Note:** Tenant group users can create a plan group with the same name as plan groups created by users in the Administrators group, System group, and Tenant group. Users in the Administrators and System groups cannot create a plan group with the same name as an existing plan group.
3. **Add Plan(s) to Group** – Adds plans to the plan group and manages your existing plans. Click **Add Plans** on the ribbon to enter the **Add Plan(s)** interface.

   ***Note:** If you have too many plans, DocAve recommends you create multiple plan groups instead of adding all of the plans to one plan group.

   Configure the following settings:

   - **Module** – Select the module whose plans you want to add to the plan group. Select one module from the **Module** drop-down list. All of the previously saved plans of the selected module are displayed in the corresponding tab.

     Now the plans from **Content Manager**, **Deployment Manager**, **Migration**, **Replicator**, **Granular Backup** and **Platform Backup** modules are available to be added in a plan group.

     Choose a tab and perform the following actions:

     ***Note**: When you are viewing or editing a plan in the corresponding interface, the plan group window will be minimized to the bottom-left of your screen. You can maximize it when you finish viewing or editing.

- **Create a New Plan** – Creates a new plan for the selected tab. After clicking this button, the corresponding product interface appears for you to create a new plan.
- **View Details** – Views detailed information of the selected plan. After clicking this button, the **View Details** interface in the plan manager of the corresponding module appears for you to view the detailed plan settings.

  ***Note:** Only **Content Manager**, **Migration**, **Granular Backup**, and **Platform Backup** modules are supported for **View Details**.
- **Edit** – Edits the saved settings of the selected plan. After clicking this button, the **Edit** interface in the plan manager of the corresponding module appears for you to edit the settings of the specified plan.
- **Refresh** – Refreshes the information displayed in the selected tab. Newly created plans can be displayed and the information of the modified plans will be updated.
- **Add to Group** – Adds the selected plans to the plan group you are configuring. The same plan can be added to the same plan group as many times as you wish.

  ***Note**: When you want to add multiple plans to the plan group, only click this button after you have selected all of the desired plans in the corresponding tabs.
- **Cancel** – Cancels the operation to go back to the **Add Plan(s) to Group** step.

  After you go back to the **Add Plan(s) to Group** step, you can view all of the plans which have already been added to the plan group. Select one plan and click **View Details** on the ribbon to view its detailed information, click **Edit** to edit its configuration, or click **Remove** to delete it from the current plan group you are creating. You can also change the order of the listed plans by selecting the order manually from the drop-down list in the **Order** column.

  After you are satisfied with the settings, click **Next** on the ribbon or the **Next** button to go to the next step.

4. **Advanced –** Configure advanced settings for the plan group:
   - **How would you like to run the plans in the group? –** Choose a group type to select how to run the plans in the plan group. Select Sequential or Parallel as the group type of the plan group.
     - **Sequential** – Runs the plans one by one according to their order in the plan group.
     - **Parallel** – Runs the plans in one plan group simultaneously according to their order in the plan group and the specified **Concurrent Plans** count.
   - **What jobs should influence the outcome of the plan group? –** This field is available when you select **Sequential** as the group type in the **How would you like to run the**

plans in the group field. Select the **Skip the subsequent jobs when the jobs with the following statuses appear** checkbox, and then select **Failed**, **Paused**, **Skipped**, **Stopped**, or **Finished with Exception** by selecting the corresponding checkboxes from the drop-down list. When jobs in this plan group complete with the selected statuses appear, the following plans in this group will be skipped.

- **How many plans would you like to run simultaneously?** – This field is available when you select **Parallel** as the group type in the **How would you like to run the plans in the group** field. Enter the number of the concurrent plans by entering a positive integer in the **Plan count** text box. The default concurrent plan number is 5, which means as many as 5 plans can be run simultaneously; all of the other plans with the order larger than 5 will wait until any of the 5 former plans is completed, and then the plan with the smaller order will be run first. When using this group type, the status of jobs in the plan group will not affect the execution of each other.

  ***Note:** For File System Migration, DocAve recommends you run at most 7 plans simultaneously to maximize efficiency.

5. Click **Next** on the ribbon or the **Next** button to go to the next step.
6. **Schedule** – Configure the schedule settings for the plan group by choosing one of the following options:

   - **Schedule –** Configure the schedule settings for the plan group by choosing one of the following options:

     - **No schedule** – Do not configure a schedule for the plan group.
     - **Configure the schedule myself** – Customize schedules for the plan group in the **Schedule Settings** field. To preview the added schedules, click **Calendar View** to view them by **Day**, by **Week**, or by **Month** in a pop-up calendar. To configure a new schedule for the plan group, click **Add Schedule** and refer to Configuring the Add Schedule Interface section for more information.

     In the **Summary** table, you can view the schedules you configured. To delete an existing schedule, click the delete ( ) button.

   - **Would you like to run all of the plans in the plan group according to the plan group's schedule?** – Select the **Disable the schedule for each plan and run plans according to the plan group's schedule** checkbox to disable the schedule for each plan in the plan group and run the plans according to the plan group's schedule.

7. Click **Next** on the ribbon or the **Next** button to go to the next step.
8. **Overview** – Review and edit the plan group settings on this page.

   - To edit settings, click the **Edit** link above the section you want to change.
   - To save the configuration, click the **Finish** button. If you want to run the plan groups job now, select **Finish and Run Now**. If you do not want to run the job immediately, select **Finish**.

Configuring the Add Schedule Interface

To configure the **Add Schedule** interface, complete the following steps:

- **Type** – Select the time unit of the time interval for this schedule from **By hour**, **By day**, **By week**, or **By month**.
- **Schedule Settings** – Configure the frequency of the time interval for this schedule by entering a positive integer in the text box. If you want to set up a more specific schedule, select the **Advanced** checkbox, and refer to the instructions below.

  If you select **By hour**, select one of the following options and configure its settings:

  - **Specify production time**: **From __ to __** – Select the production time. It will run the plan groups in the selected production time frame.

    ***Note**: All plan group jobs that started within this time frame will finish even if the end time is reached.

  - **Select time below** – Select the time you want to run the plan group. To add several time points, click **Add**.

  If you select **By Day**, enter the frequency in terms of days into the text box.

  If you select **By week**, configure the following settings:

  - **Every __ week(s)** – Enter the frequency **in** terms of weeks.
  - **On __** – Select **the** days of the week to run the plan group on.

  If you select **By month**, select one of the following options and configure its settings:

  - **On day __ of __** – Select the day of the specific month(s) to run the plan group. For example, if you select **On day 3 of January** and **July**, the plan groups will run on the third of January and July.
  - **Day __ of every __ month(s)** – Select the day of the month, and frequency in terms of months to run the plan group on. For **example**, if you select **Day 3 of every 3 month(s)**, the plan groups will run every three months, on the third of the month.
  - **The __ __of every __ month(s)** – Select on which occurrence of what day(s) of the month, and the frequency in terms of months to **run** the plan groups. For example, if you select **The First Monday of every 3 month(s)**, the plan groups will run every three months, on the first Monday of the month.
  - **The __ __ of __** – Select on which occurrence of which day(s) of which month to run the plan groups. For example, if you select **The First Monday of January** and **July**, the plan groups will run on the first Monday of January and July.
  - **Range of Recurrence** – Select the **Start time** for plan group jobs. Select one of the following options for the end time, and configure its settings:

        - **No end date** – The plan groups will run on the configured schedule until you manually end it.
        - **End after __ occurrence(s)** – The plan groups will stop running after the number of times you enter here.
        - **End by __** – The plan groups will end running on the date and time you select here.
    - **Default Settings** – The default settings on how to run plans in the plan groups for each module. Click **Edit** to customize the settings. Refer to Configuring the Default Settings Section for more information.

When you are finished configuring the new schedule you wish to add, click **Save** to save, or click **Cancel** to close the Add Schedule interface without saving.

Configuring the Default Settings Section

Refer to this section on how to configure the **Default Settings** section. The default settings for each module are:

- **Granular Backup** – The default **Option** for all of the Granular Backup plans is **Full Backup**.
- **Platform Backup** – The default **Option** for all of the Platform Backup plans is **Full Backup**, the default **Restore Granularity Level** for all of the Platform Backup plans is **Site Collection Level**, and the default **Job Report** for all of the Platform Backup plans is **Simplified**.
- **SharePoint Migration** – The default **Option** for all of the SharePoint Migration plans is **Full migration**, the default **Container Level Conflict Resolution** for all of the SharePoint Migration plans is **Skip**, the default **Check Lower Objects for Conflicts** for all of the SharePoint Migration plans is **Yes,** and the default **Content Level Conflict Resolution** for all of the SharePoint Migration plans is **Skip**.
- **Non-SharePoint Migration** – The default **Option** for all of the Non-SharePoint Migration plans is **Full migration**, the default **Container Level Conflict Resolution** for all of the Non-SharePoint Migration plans is **Merge**, the default **Check Lower Objects for Conflicts** for all of the Non-SharePoint Migration plans is **Yes,** and the default **Content Level Conflict Resolution** for all of the Non- SharePoint Migration plans is **Overwrite**.
- **Replicator** – The default **Option** for all of the Granular Backup plans is **Full Replication**.

Click the **Edit** link to edit the settings. You will be brought to the **Edit** interface.

To edit the settings for each module, click the corresponding tab:

- **Granular Backup** – Select the option from the drop-down list to configure the **Option** for all of the Granular Backup plans.
    - **Full Backup** – A full backup of the selected source.

- **Incremental Backup** – A partial backup backs up only the content that has been updated since the last backup, whether it's Full, Incremental, or Differential.
- **Differential Backup** – A partial backup backs up only the data that has been updated since the last full backup.

- **Platform Backup** – Configures the settings of **Option**, **Restore Granularity Level**, **Verify Database Backup Data**, **Check Agent Account Permissions for Backup**, **Job Report**, **Back up Web Front-End Servers in Parallel**, **Generate Index Method**, **Run Command with Operation**, **Back up Stub Database for Selected Scope**, **Back up BLOB for Selected Scope**, and **Job Time Limit**. For more information, refer to the DocAve Platform Backup and Restore User Guide.
- **SharePoint Migration** – Configure the migration type and the conflict resolution for all of the SharePoint Migration plans.
  - **Option** – Select the migration type for all of the SharePoint Migration plans.
    - **Full migration** – Migrates all contents from the source node to the destination node according to the profile.
    - **Incremental migration** – Migrates only the modified content (add and modify) to the destination based on content or time.

      ***Notes:** The **Incremental Type** cannot be configured here. If desired, configure the incremental type for each plan.
  - **Conflict Resolution** – Select the conflict resolution when the item name in the source SharePoint environment conflicts with an existing item name in the destination SharePoint environment. For **Container Level**, the conflict resolutions provided are **Merge** and **Skip**. **Merge** requires you to check lower objects for conflicts, and configure content level conflict resolution. **Skip** provides the configuration of the **Content Level** resolution optional. For more information on Conflict Resolution, refer to the DocAve SharePoint Migration User Guide.
- **Non-SharePoint Migration** – Configure the migration type, conflict resolution, and job status option for all of the Non-SharePoint Migration plans.
  - **Option** – Select the migration type for all of the Non-SharePoint Migration plans.
    - **Full migration** – Migrates all contents from the source node to the destination node according to the profile.
    - **Incremental migration** – Migrates only the modified content (add and modify) to the destination.
  - **Conflict Resolution** – Select the conflict resolution when the object name in the source environment conflicts with an existing object name in the destination SharePoint environment. For **Container Level**, the conflict resolutions provided are **Merge** and **Skip**. **Merge** requires you to check lower objects for conflicts, and configure content level conflict resolution. **Skip** provides the optional

configuration of the **Content Level** resolution. For more information on Conflict Resolution, refer to the corresponding migration user guide.

***Note:** If you select **Incremental migration** in the **Option** section, the **Remigrate the objects whose metadata/securities failed to be migrated in the last migration job** checkbox appears. If desired, select this checkbox to remigrate the objects whose metadata/securities failed to be migrated in the last migration job.

- **Job Status Option** – Choose whether to take the metadata/security exceptions into consideration for the Lotus Notes migration job status. If the content metadata or security fails to be migrated and you select the **Ignore metadata/security exceptions** checkbox, the migration job status will be **Finished**. Otherwise, the job status will be **Finished with Exceptions**.

- **Replicator** – Choose the replication mode for all of the Replicator plans.
  - **Options – Full replication** replicates all of the source content to the destination, while **Incremental Replication** only replicates the modified content (**Add**, **Delete**, and **Modify**) since last incremental or full replication. If selecting **Incremental Replication**, the following options come enabled.
  - **Modifications** – Choose whether or not to replicate the medications since last jobs.
  - **Deletions** – Choose whether or not to replicate the deletions since last job.
  - **Reference Time** – Choose whether or not to replicate contents created or modified at an entered interval. If you choose to use a reference time, enter the time to replicate contents created or modified. Enter an integer into the text box and select **Minute(s)**, **Hour(s)**, or **Day(s)** from the drop-down list.

*Note: It is recommended entering a reference time when the recurrence schedule configured in Range of Recurrence is End after 1 occurrence.

Appendix A: Examples of Filter Policies

***Note**: The **Matches Regular Expression** and **Does Not Match Regular Expression** conditions are case sensitive. None of the other conditions are case sensitive.

Site Collection Level

Rule	Condition	Value	Result
URL	Contains	test	The site collection whose URL contains test will be filtered and included in the result. For example, http://webapp:20000/sites/test and http://webapp:20000/sites/testA will be filtered and included in the result.
	Does Not Contain	test	The site collection whose URL does not contain test will be filtered and included in the result. For example, http://spapp:20000/sites/AP will be filtered and included in the result.
	Equals	http://webapp:20000/sites/test	The site collection whose URL is http://webapp:20000/sites/test will be filtered and included in the result.
	Does Not Equal	http://webapp:20000/sites/test	The site collection whose URL is not http://webapp:20000/sites/test will be filtered and included in the result.
	Matches	http://tes*collectionA	The site collection whose URL begins with http://tes and ends with collectionA will be filtered and included in the result. For example, http://tesABC:11111/sitecollectionA will be filtered and included in the result.

Rule	Condition	Value	Result
		http://test:20000/sites/sitecollecti?nA	The site collection whose URL is the same as http://test:20000/sites/sitecollecti?nA except character ? will be filtered and included in the result. For example, http://test:20000/sites/sitecollectionA and http://test:20000/sites/sitecollectiBnA will both be filtered and included in the result.
	Does Not Match	http://tes*collectionA	All the site collections except those whose URLs begin with http://tes and end with collectionA will be filtered and included in the result. For example, http://webapp:20000/sites/test will be filtered and included in the result.
		http://test:20000/sites/sitecollecti?nA	All the site collections except those whose URLs are the same as http://test:20000/sites/sitecollecti?nA except character ? will be filtered and included in the result. For example, http://webapp:20000/sites/test will be filtered and included in the result.
	Matches Regular Expression	http://test:20000/sites/[A-Z]+	All the site collections who's URLs consist of the following two parts will be filtered and included in the result: the first part is http://test:20000/sites/ and the second part contains one or more capital letters. For example, http://test:20000/sites/A will be filtered and included in the result.
	Does Not Match Regular Expression	http://test:20000/sites/[A-Z]+	All the site collections except those who's URLs consist of the following two parts will be filtered and included in the result: the first part is http://test:20000/sites/ and the second part contains one or more capital letters. For example,

Rule	Condition	Value	Result
			http://test:20000/sites/01 will be filtered and included in the result.
Title	Contains	test	The site collection whose title contains test will be filtered and included in the result.
	Does Not Contain	test	The site collection whose title does not contain test will be filtered and included in the result.
	Equals	test	The site collection whose title is test will be filtered and included in the result.
	Does Not Equal	test	The site collection whose title is not test will be filtered and included in the result.
	Matches	te*t	The site collection whose title begins with te and ends with t will be filtered and included in the result. For example, teABct will be filtered and included in the result.
		te?t	The site collection whose title is the same as te?t except character ? will be filtered and included in the result. For example, test will be filtered and included in the result.
	Does Not Match	te*t	All the site collections except those whose titles begin with te and end with t will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
		te?t	All the site collections except those whose titles are the same as te?t except character ? will be filtered and included in the result. For example, DocAve will be filtered and included in the result.

Rule	Condition	Value	Result
	Matches Regular Expression	[A-Z]+	All the site collections whose titles contain one or more capital letters will be filtered and included in the result. For example, AB will be filtered and included in the result.
	Does Not Match Regular Expression	[A-Z]+	All the site collections except those whose titles contain one or more capital letters will be filtered and included in the result. For example, 123 will be filtered and included in the result.
Modified Time	Before	11/11/2011 12:15	The site collection which is modified before 12:15:50 11/11/2011 will be filtered and included in the result.
	After	11/11/2011 12:15	The site collection which is modified after 12:15:50 11/11/2011 will be filtered and included in the result.
	On	11/11/2011	The site collection which is modified on 11/11/2011 will be filtered and included in the result.
	Within	5 Days	The site collection which is modified in last 5 days will be filtered and included in the result.
	Older Than	5 Days	The site collection which is modified 5 days ago will be filtered and included in the result.
Created Time	Before	11/11/2011 12:15	The site collection which is created before 12:15:50 11/11/2011 will be filtered and included in the result.
	After	11/11/2011 12:15	The site collection which is created after 12:15:50 11/11/2011 will be filtered and included in the result.

Rule	Condition	Value	Result
	On	11/11/2011	The site collection which is created on 11/11/2011 will be filtered and included in the result.
	Within	5 Days	The site collection which is created in last 5 days will be filtered and included in the result.
	Older Than	5 Days	The site collection which is created 5 days ago will be filtered and included in the result.
Primary Administrator	Contains	test	The site collection whose creator's NoPrefixLoginName/LoginName/Title contains test will be filtered and included in the result.
	Equals	test\user	The site collection whose creator's NoPrefixLoginName/LoginName/Title is test\user will be filtered and included in the result.
Template Name	Contains	Team	The site collection whose template name contains Team will be filtered and included in the result. For example, Team Site will be filtered and included in the result.
	Does Not Contain	Team	The site collection whose template name does not contain Team will be filtered and included in the result. For example, Blank Site will be filtered and included in the result.
	Equals	Blank Site	The site collection whose template name is Blank Site will be filtered and included in the result.
	Does Not Equal	Blank Site	The site collection whose template name is not Blank Site will be filtered and included in the result.

Rule	Condition	Value	Result
	Matches	B*Workspace	The site collection whose template name begins with B and ends with Workspace will be filtered and included in the result. For example, Basic Meeting Workspace and Blank Meeting Workspace will both be filtered and included in the result.
		Bl?g	The site collection whose template name is the same as Bl?g except character ? will be filtered and included in the result. For example, Blog will be filtered and included in the result.
	Does Not Match	B*Workspace	All the site collections except those whose templates' names begin with B and ends with Workspace will be filtered and included in the result. For example, Team Site be filtered and included in the result.
		Bl?g	All the site collections except those whose templates' names are the same as Bl?g except character ? will be filtered and included in the result. For example, Team Site will be filtered and included in the result.
	Matches Regular Expression	[A-Z]+	All the site collections whose template names contain one or more capital letters will be filtered and included in the result. For example, AB will be filtered and included in the result.
	Does Not Match Regular Expression	[A-Z]+	All the site collections except those whose template names contain one or more capital letters will be filtered and included in the result. For example, 123 will be filtered and included in the result.

Rule	Condition	Value	Result
Template ID	Contains	STS#	The site collection whose template ID contains STS# will be filtered and included in the result. For example, STS#0 (Team Site) will be filtered and included in the result.
	Equals	STS#0	The site collection whose template ID is STS#0 will be filtered and included in the result. Refer to Appendix B for more detailed information of Template ID.
Custom Property: Text	Contains	test	The site collection whose Text property contains test will be filtered and included in the result.
	Does Not Contain	test	The site collection whose Text property does not contain test will be filtered and included in the result.
	Equals	test	The site collection whose Text property is test will be filtered and included in the result.
	Does Not Equal	test	The site collection whose Text property is not test will be filtered and included in the result.
	Matches	te*t	The site collection whose Text property begins with te and ends with t will be filtered and included in the result. For example, teABct will be filtered and included in the result.
		te?t	The site collection whose Text property is the same as te?t except character ? will be filtered and included in the result. For example, test will be filtered and included in the result.

Rule	Condition	Value	Result
	Does Not Match	te*t	All the site collections except those whose Text property begins with te and ends with t will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
		te?t	All the site collections except those whose Text property is the same as te?t except character ? will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
	Matches Regular Expression	[A-Z]+	All the site collections whose Text properties contain one or more capital letters will be filtered and included in the result. For example, AB will be filtered and included in the result.
	Does Not Match Regular Expression	[A-Z]+	All the site collections except those whose Text properties contain one or more capital letters will be filtered and included in the result. For example, 123 will be filtered and included in the result.
Custom Property: Number	>=	5	The site collection whose Number property is not smaller than 5 will be filtered and included in the result. For example, 8 will be filtered and included in the result.
	<=	5	The site collection whose Number property is not bigger than 5 will be filtered and included in the result. For example, 2 will be filtered and included in the result.
	=	5	The site collection whose Number property is 5 will be filtered and included in the result.

Rule	Condition	Value	Result
Custom Property: Yes/No	Equals	Yes	The site collection whose Choice property is Yes will be filtered and included in the result.
Custom Property: Date and Time	Before	11/11/2011 12:15	The site collection whose Date property is before 12:15:50 11/11/2011 will be filtered and included in the result.
	After	11/11/2011 12:15	The site collection whose Date property is after 12:15:50 11/11/2011 will be filtered and included in the result.
	On	11/11/2011 12:15	The site collection whose Date property is on 12:15:50 11/11/2011 will be filtered and included in the result.
	Within	5 Days	The site collection whose Date property is in last 5 days will be filtered and included in the result.
	Older Than	5 Days	The site collection whose Date property is 5 days ago will be filtered and included in the result.

Site Level

Rule	Condition	Value	Result
URL	Contains	test	The site whose URL contains test will be filtered and included in the result. For example, http://webapp:20000/sites/test and http://webapp:20000/sites/testA will be filtered and included in the result.

Rule	Condition	Value	Result
	Does Not Contain	test	The site whose URL does not contain test will be filtered and included in the result. For example, http://spapp:20000/sites/AP will be filtered and included in the result.
	Equals	http://webapp:20000/sites/test	The site whose URL is http://webapp:20000/sites/test will be filtered and included in the result.
	Does Not Equal	http://webapp:20000/sites/test	The site whose URL is not http://webapp:20000/sites/test will be filtered and included in the result.
	Matches	http://tes*collectionA	The site whose URL begins with http://tes and ends with collectionA will be filtered and included in the result. For example, http://tesABC:11111/sitecollectionA will be filtered and included in the result.
		http://test:20000/sites/sitecollecti?nA	The site whose URL is the same as http://test:20000/sites/sitecollecti?nA except character ? will be filtered and included in the result. For example, http://test:20000/sites/sitecollectionA and http://test:20000/sites/sitecollectiBnA will both be filtered and included in the result.
	Does Not Match	http://tes*collectionA	All the sites except those whose URLs begin with http://tes and end with collectionA will be filtered and included in the result. For example, http://webapp:20000/sites/test will be filtered and included in the result.

Rule	Condition	Value	Result
		http://test:20000/sites/sitecollecti?nA	All the sites except those whose URLs are the same as http://test:20000/sites/sitecollecti?nA except character ? will be filtered and included in the result. For example, http://webapp:20000/sites/test will be filtered and included in the result.
	Matches Regular Expression	http://test:20000/sites/[A-Z]+	All the sites whose URLs consist of the following two parts will be filtered and included in the result: the first part is http://test:20000/sites/ and the second part contains one or more capital letters. For example, http://test:20000/sites/A will be filtered and included in the result.
	Does Not Match Regular Expression	http://test:20000/sites/[A-Z]+	All the sites except those who's URLs consist of the following two parts will be filtered and included in the result: the first part is http://test:20000/sites/ and the second part contains one or more capital letters. For example, http://test:20000/sites/01 will be filtered and included in the result.
Title	Contains	test	The site whose title contains test will be filtered and included in the result.
	Does Not Contain	test	The site whose title does not contain test will be filtered and included in the result.
	Equals	test	The site whose title is test will be filtered and included in the result.
	Does Not Equal	test	The site whose title is not test will be filtered and included in the result.

Rule	Condition	Value	Result
	Matches	te*t	The site whose title begins with te and ends with t will be filtered and included in the result. For example, teABct will be filtered and included in the result.
		te?t	The site whose title is the same as te?t except character ? will be filtered and included in the result. For example, test will be filtered and included in the result.
	Does Not Match	te*t	All the sites except those whose titles begin with te and end with t will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
		te?t	All the sites except those whose titles are the same as te?t except character ? will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
	Matches Regular Expression	[A-Z]+	All the sites whose titles contain one or more capital letters will be filtered and included in the result. For example, AB will be filtered and included in the result.
	Does Not Match Regular Expression	[A-Z]+	All the sites except those whose titles contain one or more capital letters will be filtered and included in the result. For example, 123 will be filtered and included in the result.
Modified Time	Before	11/11/2011 12:15	The site which is modified before 12:15:50 11/11/2011 will be filtered and included in the result.

Rule	Condition	Value	Result
	After	11/11/2011 12:15	The site which is modified after 12:15:50 11/11/2011 will be filtered and included in the result.
	On	11/11/2011 12:15	The site which is modified on 12:15:50 11/11/2011 will be filtered and included in the result.
	Within	5 Days	The site which is modified in last 5 days will be filtered and included in the result.
	Older Than	5 Days	The site which is modified 5 days ago will be filtered and included in the result.
Created Time	Before	11/11/2011 12:15	The site which is created before 12:15:50 11/11/2011 will be filtered and included in the result.
	After	11/11/2011 12:15	The site which is created after 12:15:50 11/11/2011 will be filtered and included in the result.
	On	11/11/2011	The site which is created on 11/11/2011 will be filtered and included in the result.
	Within	5 Days	The site which is created in last 5 days will be filtered and included in the result.
	Older Than	5 Days	The site which is created 5 days ago will be filtered and included in the result.
Created By	Contains	test	The site whose creator's NoPrefixLoginName/LoginName/Title contains test will be filtered and included in the result. For example, the sites that are created by **test\user** will be filtered and included in the result.
	Equals	test\user	The site whose creator's NoPrefixLoginName/LoginName/Title is test\user will be filtered and included in the result.

Rule	Condition	Value	Result
Template Name	Contains	Team	The site whose template name contains Team will be filtered and included in the result. For example, Team Site will be filtered and included in the result.
	Does Not Contain	Team	The site whose template name does not contain Team will be filtered and included in the result. For example, Blank Site will be filtered and included in the result.
	Equals	Blank Site	The site whose template name is Blank Site will be filtered and included in the result.
	Does Not Equal	Blank Site	The site whose template name is not Blank Site will be filtered and included in the result.
	Matches	B*Workspace	The site whose template name begins with B and ends with Workspace will be filtered and included in the result. For example, Basic Meeting Workspace and Blank Meeting Workspace will both be filtered and included in the result.
		Bl?g	The site whose template name is the same as Bl?g except character ? will be filtered and included in the result. For example, Blog will be filtered and included in the result.
	Does Not Match	B*Workspace	All the sites except those whose templates' names begin with B and ends with Workspace will be filtered and included in the result. For example, Team Site be filtered and included in the result.

Rule	Condition	Value	Result
		Bl?g	All the sites except those whose templates' names are the same as Bl?g except character ? will be filtered and included in the result. For example, Team Site will be filtered and included in the result.
	Matches Regular Expression	[A-Z]+	All the sites whose template names contain one or more capital letters will be filtered and included in the result. For example, AB will be filtered and included in the result.
	Does Not Match Regular Expression	[A-Z]+	All the sites except those whose template names contain one or more capital letters will be filtered and included in the result. For example, 123 will be filtered and included in the result.
Template ID	Contains	STS#	The site whose template ID contains STS# will be filtered and included in the result. For example, STS#0 (Team Site) will be filtered and included in the result.
	Equals	STS#0	The site whose template ID is STS#0 will be filtered and included in the result. Refer to Appendix B for more detailed information of Template ID.
Custom Property: Text	Contains	test	The site whose Text property contains test will be filtered and included in the result.
	Does Not Contain	test	The site whose Text property does not contain test will be filtered and included in the result.
	Equals	test	The site whose Text property is test will be filtered and included in the result.
	Does Not Equal	test	The site whose Text property is not test will be filtered and included in the result.

Rule	Condition	Value	Result
	Matches	te*t	The site whose Text property begins with te and ends with t will be filtered and included in the result. For example, teABct will be filtered and included in the result.
		te?t	The site whose Text property is the same as te?t except character ? will be filtered and included in the result. For example, test will be filtered and included in the result.
	Does Not Match	te*t	All the sites except those whose Text property begins with te and ends with t will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
		te?t	All the sites except those whose Text property is the same as te?t except character ? will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
	Matches Regular Expression	[A-Z]+	All the sites whose Text properties contain one or more capital letters will be filtered and included in the result. For example, AB will be filtered and included in the result.
	Does Not Match Regular Expression	[A-Z]+	All the sites except those whose Text properties contain one or more capital letters will be filtered and included in the result. For example, 123 will be filtered and included in the result.
Custom Property: Number	>=	5	The site whose Number property is not smaller than 5 will be filtered and included in the result. For example, 8 will be filtered and included in the result.

Rule	Condition	Value	Result
	<=	5	The site whose Number property is not bigger than 5 will be filtered and included in the result. For example, 2 will be filtered and included in the result.
	=	5	The site whose Number property is 5 will be filtered and included in the result.
Custom Property: Yes/No	Equals	Yes	The site whose Choice property is Yes will be filtered and included in the result.
Custom Property: Date and Time	Before	11/11/2011 12:15	The site whose Date property is before 12:15:50 11/11/2011 will be filtered and included in the result.
	After	11/11/2011 12:15	The site whose Date property is after 12:15:50 11/11/2011 will be filtered and included in the result.
	On	11/11/2011	The site whose Date property is on 11/11/2011 will be filtered and included in the result.
	Within	5 Days	The site whose Date property is in last 5 days will be filtered and included in the result.
	Older Than	5 Days	The site whose Date property is 5 days ago will be filtered and included in the result.

List/Library Level

Rule	Condition	Value	Result
Name	Contains	test	The list/library whose name contains test will be filtered and included in the result.

Rule	Condition	Value	Result
	Does Not Contain	test	The list/library whose name does not contain test will be filtered and included in the result.
	Equals	test	The list/library whose name is test will be filtered and included in the result.
	Does Not Equal	test	The list/library whose name is not test will be filtered and included in the result.
	Matches	te*t	The list/library whose name begins with te and ends with t will be filtered and included in the result. For example, teABct will be filtered and included in the result.
		te?t	The list/library whose name is the same as te?t except character ? will be filtered and included in the result. For example, test will be filtered and included in the result.
	Does Not Match	te*t	All the lists/libraries except those whose names begin with te and end with t will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
		te?t	All the lists/libraries except those whose names are the same as te?t except character ? will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
	Matches Regular Expression	[A-Z]+	All the lists/libraries whose names contain one or more capital letters will be filtered and included in the result. For example, AB will be filtered and included in the result.
	Does Not Match Regular Expression	[A-Z]+	All the lists/libraries except those whose names contain one or more capital letters will be filtered and included in the result. For

Rule	Condition	Value	Result
			example, 123 will be filtered and included in the result.
Modified Time	Before	Refer to the same filter rule in Site Collection Level.	
	After		
	On		
	Within		
	Older Than		
Created Time	Before	Refer to the same filter rule in Site Collection Level.	
	After		
	On		
	Within		
	Older Than		
Created By	Contains	Refer to the same filter rule in Site Level.	
	Equals		
Template Name	Contains	Refer to the same filter rule in Site Collection Level.	
	Does Not Contain		
	Equals		
	Does Not Equal		
	Matches		
	Does Not Match		
	Matches Regular Expression		
	Does Not Match Regular Expression		
Template ID	Equals	Refer to the same filter rule in Site Collection Level.	
	Does Not Equal		
Columns ***Note:** To filter the list/library according to	Contains	Text	The list/library that contains the column whose display name is Text will be filtered and included in the result.
		[Text]	The list/library that contains the column whose internal name is Text will be filtered and included in the result.

Rule	Condition	Value	Result
the internal name of the column, enter the internal name of the column in the bracket.	Does Not Contain	Text	The list/library that does not contain the column whose display name is Text will be filtered and included in the result.
		[Text]	The list/library that does not contain the column whose internal name is Text will be filtered and included in the result.
Content Type: Name	Contains	Test	The list/library that contains the content type whose name is Test will be filtered and included in the result.
	Does Not Contain	Test	The list/library that does not contain the content type whose name is Test will be filtered and included in the result.
Content Type: ID	Contains	0x007874566ED32546ABE3B1BC74A7D5F8	The list/library that contains the content type whose ID is 0x007874566ED32546ABE3B1BC74A7D5F8 will be filtered and included in the result.
	Does Not Contain	0x007874566ED32546ABE3B1BC74A7D5F8	The list/library that does not contain the content type whose ID is 0x007874566ED32546ABE3B1BC74A7D5F8 will be filtered and included in the result.
Custom Property: Text	Contains	Refer to the same filter rule in Site Collection Level.	
	Does Not Contain		
	Equals		
	Does Not Equal		
	Matches		
	Does Not Match		
	Matches Regular Expression		
	Does Not Match Regular Expression		
Custom Property: Number	>=	Refer to the same filter rule in Site Collection Level.	
	<=		
	=		
Custom Property: Yes/No	Equals	Refer to the same filter rule in Site Collection Level.	
Custom Property: Date and Time	Before	Refer to the same filter rule in Site Collection Level.	
	After		

Rule	Condition	Value	Result
	On		
	Within		
	Older Than		

Folder Level

Rule	Condition	Value	Result
Name	Contains	Refer to the same filter rule in List/Library Level.	
	Does Not Contain		
	Equals		
	Does Not Equal		
	Matches		
	Does Not Match		
	Matches Regular Expression		
	Does Not Match Regular Expression		
Modified Time	Before	Refer to the same filter rule in Site Collection Level.	
	After		
	On		
	Within		
	Older Than		
Created Time	Before	Refer to the same filter rule in Site Collection Level.	
	After		
	On		
	Within		
	Older Than		
Created By	Contains	Refer to the same filter rule in Site Level.	
	Equals		

Rule	Condition	Value	Result
Content Type: Name	Contains	Task	The folder whose content type name contains Task will be filtered and included in the result.
	Does Not Contain	Task	The folder whose content type name does not contain Task will be filtered and included in the result.
	Equals	Task	The folder whose content type name is Task will be filtered and included in the result.
	Does Not Equal	Task	The folder whose content type name is not Task will be filtered and included in the result.
	Matches	Ev*t	The folder whose content type name begins with Ev and ends with t will be filtered and included in the result. For example, Event will be filtered and included in the result.
	Does Not Match	Ta?k	The folder whose content type name is the same as Ta?k except character ? will be filtered and included in the result. For example, Task will be filtered and included in the result.
	Matches Regular Expression	Ev*t	All the folders except those whose content type names begin with Ev and end with t will be filtered and included in the result. For example, Task will be filtered and included in the result.
	Does Not Match Regular Expression	Ta?k	All the folders except those whose content type names are the same as Ta?k except character ? will be filtered and included in the result. For example, Event will be filtered and included in the result.
Content Type: ID	Contains	D5F8	The folder whose content type ID contains D5F8 will be filtered and included in the result.
	Does Not Contain	D5F8	The folder whose content type ID does not contain D5F8 will be filtered and included in the result.
	Equals	0x007874566ED32546ABE3B1BC74A7D5F8	The folder whose content type ID is 0x007874566ED32546ABE3B1BC74A7D5F8 will be filtered and included in the result.
	Does Not Equal	0x007874566ED32546ABE3B1BC74A7D5F8	The folder whose content type ID is not 0x007874566ED32546ABE3B1BC74A7D5F8 will be filtered and included in the result.

Rule	Condition	Value	Result
	Matches	0*F8	The folder whose content type ID begins with 0 and ends with F8 will be filtered and included in the result. For example, 0x007874566ED32546ABE3B1BC74A7D5F8 will be filtered and included in the result.
		0x007874566ED32546ABE3B1BC74A7D?F8	The folder whose content type ID is the same as 0x007874566ED32546ABE3B1BC74A7D?F8 except character ? will be filtered and included in the result. For example, 0x007874566ED32546ABE3B1BC74A7D5F8 will be filtered and included in the result.
	Does Not Match	0*F8	All the folders except those whose content type IDs begin with 0 and ends with F8 will be filtered and included in the result. For example, 0x007874566ED32546ABE3B1BC74A7D5F8 will be filtered and included in the result.
		0x007874566ED32546ABE3B1BC74A7D?F8	All the folders except those whose content type IDs are the same as 0x007874566ED32546ABE3B1BC74A7D?F8 except character ? will be filtered and included in the result. For example, 0x007874566ED32546ABE3B1BC74A7D5F8 will be filtered and included in the result.
	Matches Regular Expression	^0x01010072635879AE55BF4AA70560362FF4ABF8.*	All the folders whose content type IDs begin with 0x01010072635879AE55BF4AA70560362FF4ABF8 will be filtered and included in the result. For example, 0x01010072635879AE55BF4AA70560362FF4ABF8XX will be filtered and included in the result.
	Does Not Match Regular Expression	^0x01010072635879AE55BF4AA70560362FF4ABF8.*	All the folders except those whose content type names begin with 0x01010072635879AE55BF4AA70560362FF4ABF8 will be filtered and included in the result. For example, 0x007874566ED32546ABE3B1BC74A7D5F8 will be filtered and included in the result.
Column: Text	Contains	test	The folder whose Text column value contains test will be filtered and included in the result.

Rule	Condition	Value	Result
***Note:** Enter a display name or internal name of the Text column you are about to filter in the text box next to **Column: Text**. The internal name of the column must be entered in bracket. For example: [InternalName].	Does Not Contain	test	The folder whose Text column value does not contain test will be filtered and included in the result.
	Equals	test	The folder whose Text column value is test will be filtered and included in the result.
	Does Not Equal	test	The folder whose Text column value is not test will be filtered and included in the result.
	Matches	te*t	The folder whose Text column value begins with te and ends with t will be filtered and included in the result. For example, teABct will be filtered and included in the result.
		te?t	The folder whose Text column value is the same as te?t except character ? will be filtered and included in the result. For example, test will be filtered and included in the result.
	Does Not Match	te*t	All the folders except those whose Text column values begin with te and end with t will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
		te?t	All the folders except those whose Text column values are the same as te?t except character ? will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
	Matches Regular Expression	[A-Z]+	All the folders whose Text column values contain one or more capital letters will be filtered and included in the result. For example, AB will be filtered and included in the result.
	Does Not Match Regular Expression	[A-Z]+	All the folders except those whose Text column values contain one or more capital letters will be filtered and included in the result. For example, 123 will be filtered and included in the result.
Column: Number ***Note:** Enter a display name or internal name of	>=	5	The folder whose Number column value is not smaller than 5 will be filtered and included in the result. For example, 8 will be filtered and included in the result.

Rule	Condition	Value	Result
the Number column you are about to filter in the text box next to **Column: Number**. The internal name of the column must be entered in bracket. For example: [InternalName].	<=	5	The folder whose Number column value is not bigger than 5 will be filtered and included in the result. For example, 2 will be filtered and included in the result.
	=	5	The folder whose Number column value is 5 will be filtered and included in the result.
Column: Yes/No ***Note:** Enter a display name or internal name of the Choice column you are about to filter in the text box next to **Column: Yes/No**. The internal name of the column must be entered in bracket. For example: [InternalName].	Equals	Yes	The folder whose Choice column value is Yes will be filtered and included in the result.
Column: Date and Time ***Note:** Enter a display name or internal name of the Date column you are about to filter in the text box next to **Column: Date and Time**. The internal name of the column must be entered in bracket. For example: [InternalName].	Before	11/11/2011 12:15	The folder whose Date column value is before 12:15:50 11/11/2011 will be filtered and included in the result.
	After	11/11/2011 12:15	The folder whose Date column value is after 12:15:50 11/11/2011 will be filtered and included in the result.
	On	11/11/2011	The folder whose Date column value is on 11/11/2011 will be filtered and included in the result.
	Within	5 Days	The folder whose Date column value is in last 5 days will be filtered and included in the result.
	Older Than	5 Days	The folder whose Date column value is 5 days ago will be filtered and included in the result.
Custom Property: Text	Contains	Refer to the same filter rule in Site Collection Level.	
	Does Not Contain		
	Equals		

Rule	Condition	Value	Result
	Does Not Equal		
	Matches		
	Does Not Match		
	Matches Regular Expression		
	Does Not Match Regular Expression		
Custom Property: Number	>=	Refer to the same filter rule in Site Collection Level.	
	<=		
	=		
Custom Property: Yes/No	Equals	Refer to the same filter rule in Site Collection Level.	
Custom Property: Date and Time	Before	Refer to the same filter rule in Site Collection Level.	
	After		
	On		
	Within		
	Older Than		

Item Level

Rule	Condition	Value	Result
Title	Contains	test	The item whose title contains test will be filtered and included in the result.
	Does Not Contain	test	The item whose title does not contain test will be filtered and included in the result.
	Equals	test	The item whose title is test will be filtered and included in the result.
	Does Not Equal	test	The item whose title is not test will be filtered and included in the result.
	Matches	te*t	The item whose title begins with te and ends with t will be filtered and included in the result.

Rule	Condition	Value	Result
			For example, teABct will be filtered and included in the result.
		te?t	The item whose title is the same as te?t except character ? will be filtered and included in the result. For example, test will be filtered and included in the result.
	Does Not Match	te*t	All the items except those whose titles begin with te and end with t will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
		te?t	All the items except those whose titles are the same as te?t except character ? will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
	Matches Regular Expression	[A-Z]+	All the items whose titles contain one or more capital letters will be filtered and included in the result. For example, AB will be filtered and included in the result.
	Does Not Match Regular Expression	[A-Z]+	All the items except those whose titles contain one or more capital letters will be filtered and included in the result. For example, 123 will be filtered and included in the result.
Modified Time	Before	Refer to the same filter rule in Site Collection Level.	
	After		
	On		
	Within		
	Older Than		
Created Time	Before	Refer to the same filter rule in Site Collection Level.	
	After		
	On		
	Within		
	Older Than		

Rule	Condition	Value	Result
Last Accessed Time	Before	11/11/2011 12:15	The item which is last accessed before 12:15:50 11/11/2011 will be filtered and included in the result.
	After	11/11/2011 12:15	The item which is last accessed after 12:15:50 11/11/2011 will be filtered and included in the result.
	On	11/11/2011 12:15	The item which is last accessed on 12:15:50 11/11/2011 will be filtered and included in the result.
	Within	5 Days	The item which is last accessed in last 5 days will be filtered and included in the result.
	Older Than	5 Days	The item which is last accessed 5 days ago will be filtered and included in the result.
Created By	Contains	Refer to the same filter rule in Site Level.	
	Equals		
Modified By	Contains	test	The items whose modifier's NoPrefixLoginName/LoginName/Title contains test will be filtered and included in the result. For example, the items whose modifiers are test\user will be filtered and included in the result.
	Equals	test\user	The item whose modifier's NoPrefixLoginName/LoginName/Title is test\user will be filtered and included in the result.
Content Type: Name	Contains	Task	The item whose content type name contains Task will be filtered and included in the result.
	Does Not Contain	Task	The item whose content type name does not contain Task will be filtered and included in the result.
	Equals	Task	The item whose content type name is Task will be filtered and included in the result.

Rule	Condition	Value	Result
	Does Not Equal	Task	The item whose content type name is not Task will be filtered and included in the result.
	Matches	Ev*t	The item whose content type name begins with Ev and ends with t will be filtered and included in the result. For example, Event will be filtered and included in the result.
		Ta?k	The item whose content type name is the same as Ta?k except character ? will be filtered and included in the result. For example, Task will be filtered and included in the result.
	Does Not Match	Ev*t	All the items except those whose content type names begin with Ev and end with t will be filtered and included in the result. For example, Task will be filtered and included in the result.
		Ta?k	All the items except those whose content type names are the same as Ta?k except character ? will be filtered and included in the result. For example, Event will be filtered and included in the result.
	Matches Regular Expression	[A-Z]+	All the items whose content type names contain one or more capital letters will be filtered and included in the result. For example, AB will be filtered and included in the result.
	Does Not Match Regular Expression	[A-Z]+	All the items except those whose content type names contain one or more capital letters will be filtered and included in the result. For example, 123 will be filtered and included in the result.
Content Type: ID	Contains	D5F8	The item whose content type ID contains D5F8 will be filtered and included in the result.
	Does Not Contain	D5F8	The item whose content type ID does not contain D5F8 will be filtered and included in the result.

Rule	Condition	Value	Result
	Equals	0x007874566ED32546ABE3B1BC74A7D5F8	The item whose content type ID is 0x007874566ED32546ABE3B1BC74A7D5F8 will be filtered and included in the result.
	Does Not Equal	0x007874566ED32546ABE3B1BC74A7D5F8	The item whose content type ID is not 0x007874566ED32546ABE3B1BC74A7D5F8 will be filtered and included in the result.
	Matches	0*F8	The item whose content type ID begins with 0 and ends with F8 will be filtered and included in the result. For example, 0x007874566ED32546ABE3B1BC74A7D5F8 will be filtered and included in the result.
		0x007874566ED32546ABE3B1BC74A7D?F8	The item whose content type ID is the same as 0x007874566ED32546ABE3B1BC74A7D?F8 except character ? will be filtered and included in the result. For example, 0x007874566ED32546ABE3B1BC74A7D5F8 will be filtered and included in the result.
	Does Not Match	0*F8	All the items except those whose content type IDs begins with 0 and ends with F8 will be filtered and included in the result. For example, 0x007874566ED32546ABE3B1BC74A7D5F8 will be filtered and included in the result.
		0x007874566ED32546ABE3B1BC74A7D?F8	All the items except those whose content type IDs are the same as 0x007874566ED32546ABE3B1BC74A7D?F8 except character ? will be filtered and included in the result. For example, 0x007874566ED32546ABE3B1BC74A7D5F8 will be filtered and included in the result.
	Matches Regular Expression	^0x01010072635879AE55BF4AA70560362FF4ABF8.*	All the items whose content type IDs begin with 0x01010072635879AE55BF4AA70560362FF4ABF8 will be filtered and included in the result. For example,

Rule	Condition	Value	Result
			0x01010072635879AE55BF4AA70560362FF4ABF8XX will be filtered and included in the result.
	Does Not Match Regular Expression	^0x01010072635879AE55BF4AA70560362FF4ABF8.*	All the items except those whose content type names begin with 0x01010072635879AE55BF4AA70560362FF4ABF8 will be filtered and included in the result. For example, 0x007874566ED32546ABE3B1BC74A7D5F8 will be filtered and included in the result.
Column: Text ***Note:** Enter a display name or internal name of the Text column you are about to filter in the text box next to **Column: Text**. The internal name of the column must be entered in bracket. For example: [InternalName].	Contains	test	The item whose Text column value contains test will be filtered and included in the result.
	Does Not Contain	test	The item whose Text column value does not contain test will be filtered and included in the result.
	Equals	test	The item whose Text column value is test will be filtered and included in the result.
	Does Not Equal	test	The item whose Text column value is not test will be filtered and included in the result.
	Matches	te*t	The item whose Text column value begins with te and ends with t will be filtered and included in the result. For example, teABct will be filtered and included in the result.
		te?t	The item whose Text column value is the same as te?t except character ? will be filtered and included in the result. For example, test will be filtered and included in the result.
	Does Not Match	te*t	All the items except those whose Text column values begin with te and end with t will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
		te?t	All the items except those whose Text column values are the same as te?t except character ?

Rule	Condition	Value	Result
			will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
	Matches Regular Expression	[A-Z]+	All the items whose Text column values contain one or more capital letters will be filtered and included in the result. For example, AB will be filtered and included in the result.
	Does Not Match Regular Expression	[A-Z]+	All the items except those whose Text column values contain one or more capital letters will be filtered and included in the result. For example, 123 will be filtered and included in the result.
Column: Number ***Note:** Enter a display name or internal name of the Number column you are about to filter in the text box next to **Column: Number**. The internal name of the column must be entered in bracket. For example: [InternalName].	>=	5	The item whose Number column value is not smaller than 5 will be filtered and included in the result. For example, 8 will be filtered and included in the result.
	<=	5	The item whose Number column value is not bigger than 5 will be filtered and included in the result. For example, 2 will be filtered and included in the result.
	=	5	The item whose Number column value is 5 will be filtered and included in the result.
Column: Yes/No ***Note:** Enter a display name or internal name of the Choice column you are about to filter in the text box next to **Column: Yes/No**. The internal name of the column must be entered in bracket. For example: [InternalName].	Equals	Yes	The item whose Choice column value is Yes will be filtered and included in the result.
Column: Date and Time ***Note:** Enter a display name or internal name of the Date column	Before	11/11/2011 12:15	The item whose Date column value is before 12:15:50 11/11/2011 will be filtered and included in the result.

Rule	Condition	Value	Result
you are about to filter in the text box next to **Column: Date and Time**. The internal name of the column must be entered in bracket. For example: [InternalName].	After	11/11/2011 12:15	The item whose Date column value is after 12:15:50 11/11/2011 will be filtered and included in the result.
	On	11/11/2011	The item whose Date column value is on 11/11/2011 will be filtered and included in the result.
	Within	5 Days	The item whose Date column value is in last 5 days will be filtered and included in the result.
	Older Than	5 Days	The item whose Date column value is 5 days ago will be filtered and included in the result.
Workflow ***Note:** Enter the display name of the column you are about to filter in the text box next to **Workflow**.	Equals	Completed	The item associated with the Flow workflow whose status is Completed will be filtered and included in the result.
		In Progress	The item associated with the Flow workflow whose status is In Progress will be filtered and included in the result.
	Does Not Equal	In Progress	The item associated with the Flow workflow whose status is not In Progress will be filtered and included in the result. For example, Completed will be filtered and included in the result.
		Completed	The item associated with the Flow workflow whose status is not Completed will be filtered and included in the result. For example, In Progress will be filtered and included in the result.

Rule	Condition	Value	Result
Version	Latest [] Versions and Current Version	3	The item's last 4 versions will be filtered and included in the result. For example, an item has the following versions: 1.0, 2.0, 3.0, 4.0, 5.0, 6.0, then, version 3.0, 4.0, 5.0 and the current version 6.0 will be filtered and included in the result.
	Approved Versions and Current Version	N/A	All approved versions and the current version will be filtered and included in the result.
Custom Property: Text	Contains	test	The item whose Text property contains test will be filtered and included in the result.
	Does Not Contain	test	The item whose Text property does not contain test will be filtered and included in the result.
	Equals	test	The item whose Text property is test will be filtered and included in the result.
	Does Not Equal	test	The item whose Text property is not test will be filtered and included in the result.
	Matches	te*t	The item whose Text property begins with te and ends with t will be filtered and included in the result. For example, teABct will be filtered and included in the result.

Rule	Condition	Value	Result
		te?t	The item whose Text property is the same as te?t except character ? will be filtered and included in the result. For example, test will be filtered and included in the result.
	Does Not Match	te*t	All the items except those whose Text property begins with te and ends with t will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
		te?t	All the items except those whose Text property is the same as te?t except character ? will be filtered and included in the result. For example, DocAve will be filtered and included in the result.
	Matches Regular Expression	[A-Z]+	All the items whose Text properties contain one or more capital letters will be filtered and included in the result. For example, AB will be filtered and included in the result.
	Does Not Match Regular Expression	[A-Z]+	All the items except those whose Text properties contain one or more capital letters will be filtered and included in the result. For example, 123 will be filtered and included in the result.
Custom Property: Number	>=	5	The item whose Number property is not smaller than 5 will be filtered and included in the result. For example, 8 will be filtered and included in the result.
	<=	5	The item whose Number property is not bigger than 5 will be filtered and included in the result. For example, 2 will be filtered and included in the result.
	=	5	The item whose Number property is 5 will be filtered and included in the result.

Rule	Condition	Value	Result
Custom Property: Yes/No	Equals	Yes	The item whose Choice property is Yes will be filtered and included in the result.
Custom Property: Date and Time	Before	11/11/2011 12:15	The item whose Date property is before 12:15:50 11/11/2011 will be filtered and included in the result.
	After	11/11/2011 12:15	The item whose Date property is after 12:15:50 11/11/2011 will be filtered and included in the result.
	On	11/11/2011	The item whose Date property is on 11/11/2011 will be filtered and included in the result.
	Within	5 Days	The item whose Date property is in last 5 days will be filtered and included in the result.
	Older Than	5 Days	The item whose Date property is 5 days ago will be filtered and included in the result.

Document Level

Rule	Condition	Value	Result
Name	Contains	test	The document whose name contains test will be filtered and included in the result. For example, test.docx will be filtered and included in the result.
	Does Not Contain	test	The document whose name does not contain test will be filtered and included in the result. For example, DocAve.docx will be filtered and included in the result.
	Equals	test.docx	The document whose name is test.docx will be filtered and included in the result.
	Does Not Equal	test.docx	The document whose name is not test.docx will be filtered and included in the result.

Rule	Condition	Value	Result
	Matches	te*t.docx	The document whose name begins with te and ends with t.docx will be filtered and included in the result. For example, testDocAve.docx will be filtered and included in the result.
		te?t.docx	The document whose name is the same as te?t except character ? will be filtered and included in the result. For example, teAt.docx will be filtered and included in the result.
	Does Not Match	te*t.docx	All the documents except those whose names begin with te and end with t.docx will be filtered and included in the result. For example, DocAve.txt will be filtered and included in the result.
		te?t.docx	All the documents except those whose names are the same as te?t.docx except character ? will be filtered and included in the result. For example, DocAve.txt will be filtered and included in the result.
	Matches Regular Expression	[A-Z]+	All the documents whose names contain one or more capital letters will be filtered and included in the result. For example, AB will be filtered and included in the result.
	Does Not Match Regular Expression	[A-Z]+	All the documents except those whose names contain one or more capital letters will be filtered and included in the result. For example, 123 will be filtered and included in the result.
File Extension	Equals	.docx	The document whose extension equals .docx will be filtered and included in the result. For example, Sample.docx will be filtered and included in the result.
	Does Not Equal	.docx	The document whose extension does not equal .docx will be filtered and included in the

Rule	Condition	Value	Result
			result. For example, Sample.txt will be filtered and included in the result.
Size	>=	1MB	The document whose size is not smaller than 1MB will be filtered and included in the result. For example, a 2MB document will be filtered and included in the result.
	<=	1MB	The document whose size is not bigger than 5 will be filtered and included in the result. For example, a 500KB document will be filtered and included in the result.
Modified Time	Before	Refer to the same filter rule in Site Collection Level.	
	After		
	On		
	Within		
	Older Than		
Created Time	Before	Refer to the same filter rule in Site Collection Level.	
	After		
	On		
	Within		
	Older Than		
Last Accessed Time	Before	Refer to the same filter rule in Item Level.	
	After		
	On		
	Within		
	Older Than		
Created By	Contains	Refer to the same filter rule in Site Level.	
	Equals		
Modified By	Contains	Refer to the same filter rule in Item Level.	
	Equals		
Content Type: Name	Contains	Refer to the same filter rule in Item Level.	
	Does Not Contain		

Rule	Condition	Value	Result
	Equals		
	Does Not Equal		
	Matches		
	Does Not Match		
	Matches Regular Expression		
	Does Not Match Regular Expression		
Content Type: ID	Contains	Refer to the same filter rule in Item Level.	
	Does Not Contain		
	Equals		
	Does Not Equal		
	Matches		
	Does Not Match		
	Matches Regular Expression		
	Does Not Match Regular Expression		
Column: Text ***Note:** Enter a display name or internal name of the Text column you are about to filter in the text box next to **Column: Text**. The internal name of the column must be entered in bracket. For example: [InternalName].	Contains	Refer to the same filter rule in Item Level.	
	Does Not Contain		
	Equals		
	Does Not Equal		
	Matches		
	Does Not Match		
	Matches Regular Expression		
	Does Not Match Regular Expression		
Column: Number	>=	Refer to the same filter rule in Item Level.	
	<=		

Rule	Condition	Value	Result
***Note:** Enter a display name or internal name of the Number column you are about to filter in the text box next to **Column: Number**. The internal name of the column must be entered in bracket. For example: [InternalName].	=		
Column: Yes/No ***Note:** Enter a display name or internal name of the Choice column you are about to filter in the text box next to **Column: Yes/No**. The internal name of the column must be entered in bracket. For example: [InternalName].	Equals	Refer to the same filter rule in Item Level.	
Column: Date and Time ***Note:** Enter a display name or internal name of the Date column you are about to filter in the text box next to **Column: Date and Time**. The internal name of the column must be entered in bracket. For example: [InternalName].	Before After On Within Older Than		
Workflow ***Note:** Enter the display name of the column you are about to filter in the text box next to **Workflow**.	Equals Does Not Equal	Refer to the same filter rule in Item Level.	
Version	Latest [] Versions and Current Version	3	The document's last 4 versions will be filtered and included in the result. For example, if a document has the following versions: 1.0, 1.1, 2.0, 2.1, 2.2, then, version 1.1, 2.0, 2.1 and the current version 2.2 will be filtered and included in the result.

Rule	Condition	Value	Result
	Latest [] Major Versions and Current Version	3	The document's last 3 major versions will be filtered and included in the result. For example, if a document has the following versions: 1.0, 2.0, 2.1, 2.2, 3.0, 3.1, and then the major version 1.0, 2.0, 3.0, and the current version 3.1 will be filtered and included in the result.
	Major Versions and Current Version	N/A	All major versions and the current version will be filtered and included in the result.
	Approved Versions and Current Version	Refer to the same filter rule in Item Level.	
Custom Property: Text	Contains	Refer to the same filter rule in Item Level.	
	Does Not Contain		
	Equals		
	Does Not Equal		
	Matches		
	Does Not Match		
	Matches Regular Expression		
	Does Not Match Regular Expression		
Custom Property: Number	>=	Refer to the same filter rule in Item Level.	
	<=		
	=		
Custom Property: Yes/No	Equals	Refer to the same filter rule in Item Level.	
Custom Property: Date and Time	Before	Refer to the same filter rule in Item Level.	
	After		
	On		
	Within		
	Older Than		

Attachment Level

Rule	Condition	Value	Result
Name	Contains	Refer to the same filter rule in Document Level.	
	Does Not Contain		
	Equals		
	Does Not Equal		
	Matches		
	Does Not Match		
	Matches Regular Expression		
	Does Not Match Regular Expression		
File Extension	Equals	Refer to the same filter rule in Document Level.	
	Does Not Equal		
Size	>=	Refer to the same filter rule in Document Level.	
	<=		
Created Time	Before	Refer to the same filter rule in Site Collection Level.	
	After		
	On		
	Within		
	Older Than		
Last Accessed Time	Before	Refer to the same filter rule in Item Level.	
	After		
	On		
	Within		
	Older Than		
Created By	Contains	Refer to the same filter rule in Site Level.	
	Equals		
Column: Text	Contains	Refer to the same filter rule in Item Level.	

Rule	Condition	Value	Result
***Note:** Enter a display name or internal name of the Text column you are about to filter in the text box next to **Column: Text**. The internal name of the column must be entered in bracket. For example: [InternalName]. ***Note:** The column entered here is the column of the item where the attachment you are about to filter resides.	Does Not Contain Equals Does Not Equal Matches Does Not Match Matches Regular Expression Does Not Match Regular Expression		
Column: Number ***Note:** Enter a display name or internal name of the Number column you are about to filter in the text box next to **Column: Number**. The internal name of the column must be entered in bracket. For example: [InternalName]. ***Note:** The column entered here is the column of the item where the attachment you are about to filter resides.	>= <= =	Refer to the same filter rule in Item Level.	
Column: Yes/No ***Note:** Enter a display name or internal name of the Choice column you are about to filter in the text box next to **Column: Yes/No**. The internal name of the column must be entered in bracket. For example: [InternalName]. ***Note:** The column entered here is the column of the item where the attachment you are about to filter resides.	Equals	Refer to the same filter rule in Item Level.	
Column: Date and Time ***Note:** Enter a display name or internal name of the Date column you are about to	Before After On	Refer to the same filter rule in Item Level.	

Rule	Condition	Value	Result
filter in the text box next to **Column: Date and Time**. The internal name of the column must be entered in bracket. For example: [InternalName]. ***Note:** The column entered here is the column of the item where the attachment you are about to filter resides.	Within Older Than		

Appendix B: Template Name and Template ID

Refer to the table below for the detailed mappings between the Template Name and Template ID.

Template Name	Template ID
Global template	GLOBAL#0
Team Site	STS#0
Blank Site	STS#1
Document Workspace	STS#2
Basic Meeting Workspace	MPS#0
Blank Meeting Workspace	MPS#1
Decision Meeting Workspace	MPS#2
Social Meeting Workspace	MPS#3
Multipage Meeting Workspace	MPS#4
Central Admin Site	CENTRALADMIN#0
Wiki Site	WIKI#0
Blog	BLOG#0
Group Work Site	SGS#0
Tenant Admin Site	TENANTADMIN#0
Access Services Site	ACCSRV#0
Assets Web Database	ACCSRV#1
Charitable Contributions Web Database	ACCSRV#3
Contacts Web Database	ACCSRV#4
Issues Web Database	ACCSRV#6
Projects Web Database	ACCSRV#5
Document Center	BDR#0
(obsolete) Records Center	OFFILE#0
Records Center	OFFILE#1
Shared Services Administration Site	OSRV#0
PerformancePoint	PPSMASite#0
Business Intelligence Center	BICenterSite#0
SharePoint Portal Server Site	SPS#0
SharePoint Portal Server Personal Space	SPSPERS#0
Personalization Site	SPSMSITE#0
Contents area Template	SPSTOC#0
Topic area template	SPSTOPIC#0
News Site	SPSNEWS#0
Publishing Site	CMSPUBLISHING#0
Publishing Site	BLANKINTERNET#0
Press Releases Site	BLANKINTERNET#1
Publishing Site with Workflow	BLANKINTERNET#2
News Site	SPSNHOME#0
Site Directory	SPSSITES#0
Community area template	SPSCOMMU#0
Report Center	SPSREPORTCENTER#0

Template Name	Template ID
Collaboration Portal	SPSPORTAL#0
Enterprise Search Center	SRCHCEN#0
Profiles	PROFILES#0
Publishing Portal	BLANKINTERNETCONTAINER#0
My Site Host	SPSMSITEHOST#0
Enterprise Wiki	ENTERWIKI#0
Basic Search Center	SRCHCENTERLITE#0
Basic Search Center	SRCHCENTERLITE#1
FAST Search Center	SRCHCENTERFAST#0
Visio Process Repository	visprus#0

Appendix C: Hot Key Functionality

See the following sections for Control Panel and Plan Group hot key functions.

Using Hot Keys Mode in Control Panel

In order to work faster and improve your productivity, DocAve supports the hot key mode for you to perform corresponding actions quickly by only using your keyboard.

To access the hot key mode, press the **Ctrl** +**Alt** + **Z** key combination simultaneously on your keyboard while in the DocAve interface. Then press **3** to access the Control Panel.

The following sections provide lists of hot keys for the top level. Each time you want to go back to the top level after accessing the interface of lower level, press **Ctrl** + **Alt** + **Z** on the keyboard.

Manager Monitor

To access the hot key mode in the Manager Monitor interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **O** to activate the hot keys for buttons on the ribbon.

<table>
<tr><th colspan="6">Function Name and Hot Key</th></tr>
<tr><td rowspan="7">Configure</td><td rowspan="7">J</td><td>Add Cache Location</td><td>A</td><td>Save</td><td>S</td></tr>
<tr><td></td><td></td><td>Cancel</td><td>C</td></tr>
<tr><td>Edit Cache Location</td><td>E</td><td>Save</td><td>S</td></tr>
<tr><td></td><td></td><td>Cancel</td><td>C</td></tr>
<tr><td>Refresh</td><td colspan="3">R</td></tr>
<tr><td>Delete</td><td colspan="3">D</td></tr>
<tr><td>Save</td><td colspan="3">S</td></tr>
<tr><td>Cancel</td><td colspan="3">C</td></tr>
<tr><td>View Details</td><td>V</td><td>Close</td><td colspan="3">B</td></tr>
<tr><td rowspan="2">Notification Selection</td><td rowspan="2">N</td><td>Save</td><td colspan="3">S</td></tr>
<tr><td>Cancel</td><td colspan="3">C</td></tr>
<tr><td>Restart</td><td colspan="5">R</td></tr>
<tr><td>Remove</td><td colspan="5">M</td></tr>
<tr><td>Deactivate</td><td colspan="5">D</td></tr>
<tr><td>Activate</td><td colspan="5">A</td></tr>
<tr><td>Close</td><td colspan="5">X</td></tr>
</table>

Agent Monitor

To access the hot key mode in the Agent Monitor interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **M** to activate the hot keys for buttons on the ribbon.

Function Name and Hot Key			
Configure	J	Save	S
		Cancel	C
Configuration File	C		
View Details	V	Close	X
Notification Selection	N	Save	S
		Cancel	C
Restart	R		
Remove	M		
Deactivate	D		
Activate	A		
Close	X		

System Option

To access the hot key mode in the System Option interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **Y** to activate the hot keys for buttons on the ribbon.

Function Name and Hot Key							
General	G						
Security	SC						
Security Information	SI	Backup	B				
		Manage Passphrase	MP	Modify	MD	Save	S
						Cancel	C
				Cancel	C		
		Cancel	C				
Save	SE						
Close	X						

Authentication Manager

To access the hot key mode in the Authentication Manager interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **A** to activate the hot keys for buttons on the ribbon.

Function Name and Hot Key					
Windows Authentication	W	Save	S		
		Cancel	C		
AD Integration	AI	Add	A	Save	S
				Cancel	C
		Edit	ED	Save	S
				Cancel	C
		Delete	DE		
		Disable	DI		

Function Name and Hot Key					
		Enable	EN		
		Cancel	C		
ADFS Integration	AD	ADFS integration	A	Back	B
				Next	N
				Finish	F
				Cancel	C
		Add Federation Trust	F	Save	S
				Cancel	C
Close	X				

Account Manager

To access the hot key mode in the Account Manager interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **N** to activate hot keys for buttons on the ribbon.

Function Name and Hot Key								
Adding Group								
Groups	G							
Add Group	AG	Back	B					
		Next	N					
		Finish	F					
		Cancel	C					
Edit Group	E	Save	O					
		Cancel	C					
Show User(s)	S	System Group	Add User to Group	A	Save	S		
					Cancel	C		
			Remove User from Group		R			
			Cancel		C			
		Tenant Group	User-based View	U	Add User	AU	Back	B
							Next	N
							Finish	F
							Cancel	C
					Change Permission	C	Back	B
							Next	N
							Finish	F
							Cancel	C
					Remove from Group	R		

<table>
<tr><th colspan="12">Function Name and Hot Key</th></tr>
<tr><td colspan="3" rowspan="6"></td><td colspan="2" rowspan="6"></td><td rowspan="6"></td><td>Activate</td><td>AC</td><td colspan="4"></td></tr>
<tr><td>Deactivate</td><td>D</td><td colspan="4"></td></tr>
<tr><td rowspan="3">Audit Report</td><td rowspan="3">AR</td><td>Export to Datasheet</td><td>E</td></tr>
<tr><td>Output Screenshot</td><td>O</td></tr>
<tr><td>Close</td><td>X</td></tr>
<tr><td colspan="2">Close</td><td>X</td><td colspan="4"></td></tr>
<tr><td colspan="2" rowspan="3">Object-based View</td><td rowspan="3">O</td><td rowspan="2">Change Permission</td><td rowspan="2">C</td><td>Save</td><td>S</td></tr>
<tr><td>Cancel</td><td>C</td></tr>
<tr><td>Close</td><td>X</td></tr>
<tr><td colspan="3">Delete Group</td><td>D</td><td colspan="8"></td></tr>
<tr><td rowspan="5">Import in Bulk</td><td rowspan="5">B</td><td colspan="4">Download Template</td><td>D</td><td colspan="4"></td></tr>
<tr><td colspan="4">Tenant Group Template</td><td>T</td><td colspan="4"></td></tr>
<tr><td colspan="4">System Group Template</td><td>S</td><td colspan="4"></td></tr>
<tr><td colspan="4">Save</td><td>O</td><td colspan="4"></td></tr>
<tr><td colspan="4">Cancel</td><td>C</td><td colspan="4"></td></tr>
<tr><td rowspan="7">Permission Level</td><td rowspan="7">P</td><td rowspan="4">Add</td><td rowspan="4">A</td><td colspan="2" rowspan="2">Add System Permission</td><td rowspan="2">AS</td><td>Save</td><td>S</td></tr>
<tr><td>Cancel</td><td>C</td></tr>
<tr><td colspan="2" rowspan="2">Add Tenant Permission</td><td rowspan="2">AT</td><td>Save</td><td>S</td></tr>
<tr><td>Cancel</td><td>C</td></tr>
<tr><td rowspan="2">Edit</td><td rowspan="2">E</td><td>Save</td><td colspan="5">S</td></tr>
<tr><td>Cancel</td><td colspan="5">C</td></tr>
<tr><td>Delete</td><td colspan="7">D</td></tr>
<tr><td>Cancel</td><td colspan="7">C</td></tr>
<tr><td rowspan="2">Current Logon Account (s)</td><td rowspan="2">C</td><td>Log Off</td><td colspan="7">L</td></tr>
<tr><td>Cancel</td><td colspan="7">B</td></tr>
<tr><td colspan="4">Authentication Manager</td><td colspan="8">AM</td></tr>
<tr><td colspan="3">Close</td><td>X</td><td colspan="8"></td></tr>
<tr><td colspan="12">Adding User</td></tr>
<tr><td colspan="3">Users</td><td>U</td><td colspan="8"></td></tr>
<tr><td rowspan="2">Add User</td><td>A</td><td>Save</td><td colspan="9">S</td></tr>
<tr><td>U</td><td>Cancel</td><td colspan="9">C</td></tr>
<tr><td rowspan="6">View Details</td><td rowspan="6">V</td><td rowspan="2">Edit User</td><td rowspan="2">E</td><td colspan="2">Save</td><td>S</td><td colspan="6"></td></tr>
<tr><td colspan="2">Cancel</td><td>C</td><td colspan="6"></td></tr>
<tr><td>Delete User</td><td colspan="10">DU</td></tr>
<tr><td>Activate</td><td colspan="10">AC</td></tr>
<tr><td>Deactivate</td><td colspan="10">DA</td></tr>
<tr><td>Close</td><td colspan="10">X</td></tr>
<tr><td>Edit User</td><td>E</td><td>Save</td><td colspan="10">S</td></tr>
</table>

Function Name and Hot Key							
		Cancel	C				
Delete User	DU						
Activate	AC						
Deactivate	DA						
Import in Bulk	B	Download Template	D				
		Tenant Group Template	T				
		System Group Template	S				
		Save	O				
		Cancel	C				
Permission Level	P	Add	A	Add System Permission	AS	Save	S
						Cancel	C
				Add Tenant Permission	AT	Save	S
						Cancel	C
		Edit	E	Save	S		
				Cancel	C		
		Delete	D				
		Cancel	C				
Current Logon Account (s)	C	Log Off	L				
		Cancel	C				
Authentication Manager	AM						
Close	X						

License Manager

To access the hot key mode in the License Manager interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **Z** to activate the Hot Key of the buttons on the ribbon.

Function Name and Hot Key			
Import	I		
Export	E	License File	F
		License Report	R
Settings	S	Save	O
		Cancel	C
SharePoint Servers Usage	A	View Details	V
		Save	O
		Cancel	C
Close	X		

Update Manager

To access the hot key mode in the Update Manager interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **H** to activate the hot keys for buttons on the ribbon.

<table>
<tr><th colspan="6">Function Name and Hot Key</th></tr>
<tr><td rowspan="6">Manager Updates</td><td rowspan="6">M</td><td rowspan="2">View History</td><td rowspan="2">V</td><td>View Details</td><td>V</td></tr>
<tr><td>Cancel</td><td>B</td></tr>
<tr><td>Browse</td><td colspan="3">U</td></tr>
<tr><td>Install</td><td colspan="3">I</td></tr>
<tr><td>Delete</td><td colspan="3">DE</td></tr>
<tr><td>Cancel</td><td colspan="3">B</td></tr>
<tr><td rowspan="2">View History</td><td rowspan="2">V</td><td>View Details</td><td colspan="3">V</td></tr>
<tr><td>Cancel</td><td colspan="3">B</td></tr>
<tr><td rowspan="2">Update Settings</td><td rowspan="2">U</td><td>Save</td><td colspan="3">O</td></tr>
<tr><td>Cancel</td><td colspan="3">B</td></tr>
<tr><td>Close</td><td colspan="5">X</td></tr>
</table>

Agent Groups

To access the hot key mode in the Agent Groups interface press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **G** to activate the hot keys for buttons on the ribbon.

<table>
<tr><th colspan="8">Function Name and Hot Key</th></tr>
<tr><td rowspan="2">Create</td><td rowspan="2">N</td><td colspan="3">Save</td><td colspan="3">O</td></tr>
<tr><td colspan="3">Cancel</td><td colspan="3">C</td></tr>
<tr><td rowspan="3">View Details</td><td rowspan="3">O</td><td colspan="3" rowspan="3">Edit</td><td rowspan="3">E</td><td>Save</td><td>S</td></tr>
<tr><td rowspan="2">Save</td><td rowspan="2">S</td><td>Save As</td><td>A</td></tr>
<tr><td>Cancel</td><td>C</td></tr>
<tr><td colspan="3">Cancel</td><td colspan="3">C</td></tr>
<tr><td rowspan="3">Edit</td><td rowspan="3">E</td><td rowspan="2">Save</td><td rowspan="2">S</td><td>Save</td><td colspan="3">S</td></tr>
<tr><td>Save As</td><td colspan="3">A</td></tr>
<tr><td colspan="3">Cancel</td><td colspan="3">C</td></tr>
<tr><td>Delete</td><td colspan="7">D</td></tr>
<tr><td>Close</td><td colspan="7">X</td></tr>
</table>

User Notification Setting

To access the hot key mode in the User Notification Setting interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **V** to activate the hot keys for buttons on the ribbon.

<table>
<tr><th colspan="8">Function Name and Hot Key</th></tr>
<tr><td>Outgoing E-mail Settings</td><td colspan="7">O</td></tr>
<tr><td rowspan="8">Notification E-mail Settings</td><td rowspan="8">I
E</td><td rowspan="2">Create</td><td rowspan="2">N</td><td>Save</td><td colspan="3">S</td></tr>
<tr><td>Cancel</td><td colspan="3">C</td></tr>
<tr><td rowspan="3">View Details</td><td rowspan="3">V</td><td rowspan="2">Edit</td><td rowspan="2">E</td><td>Save</td><td>S</td></tr>
<tr><td>Cancel</td><td>C</td></tr>
<tr><td>Cancel</td><td colspan="3">C</td></tr>
<tr><td rowspan="2">Edit</td><td rowspan="2">E</td><td>Save</td><td colspan="3">S</td></tr>
<tr><td>Cancel</td><td colspan="3">C</td></tr>
<tr><td>Delete</td><td colspan="5">D</td></tr>
<tr><td>Set as Default Profile</td><td colspan="5">S</td></tr>
<tr><td>Close</td><td colspan="5">X</td></tr>
<tr><td>Save</td><td colspan="7">S</td></tr>
<tr><td>Close</td><td colspan="7">X</td></tr>
</table>

Job Pruning

To access the hot key mode in the Job Pruning interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **J** to activate the hot keys for buttons on the ribbon.

<table>
<tr><th colspan="4">Function Name and Hot Key</th></tr>
<tr><td>Prune Now</td><td colspan="3">P</td></tr>
<tr><td rowspan="2">Configure</td><td rowspan="2">C</td><td>Save</td><td>O</td></tr>
<tr><td>Cancel</td><td>B</td></tr>
<tr><td>Job Monitor</td><td colspan="3">J</td></tr>
<tr><td>Save</td><td colspan="3">S</td></tr>
<tr><td>Close</td><td colspan="3">X</td></tr>
</table>

Job Performance Alert

To access the hot key mode in the Job Performance Alert interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **L** to activate the hot keys for buttons on the ribbon.

<table>
<tr><th colspan="4">Function Name and Hot Key</th></tr>
<tr><td rowspan="2">Configure</td><td rowspan="2">C</td><td>Save</td><td>S</td></tr>
<tr><td>Cancel</td><td>B</td></tr>
<tr><td>Close</td><td colspan="3">X</td></tr>
</table>

Log Manager

To access the hot key mode in the Log Manager interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **B** to activate the hot keys for buttons on the ribbon.

Function Name and Hot Key					
Log Settings	L	Batch Log Settings	B	Save	S
				Cancel	B
		Save	S		
		Cancel	C		
Log Scrub	S	Import	I		
		Export	E		
		Retrieve Data	R		
		Save	S		
		Cancel	C		
Job Monitor	J				
Collect	C				
Close	X				

Registered SharePoint Sites

To access the hot key mode in the Registered SharePoint Sites interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **S** to activate the hot keys for buttons on the ribbon.

Function Name and Hot Key					
Manual Input Mode	MI				
Create	C	Save	O		
		Cancel	B		
View Details	V	Edit	E	Save	O
				Cancel	B
		Cancel	B		
Edit	E	Save	O		
		Cancel	B		
Delete	D				
Manage Site Collection	M	Add	A	Save	O
				Cancel	B
		View Details	V		
		Edit	E		
		Delete	D		
		Batch Add Site Collections	I		
		Retrieve Status	R		
		Cancel	B		

Function Name and Hot Key				
Close	X			
Scan Mode	SM			
New Group	NG	Save	O	
		Cancel	B	
Delete	D			
Add	A			
Remove	RM			
Scan	SN			
Reconnect	RC			
Save	SA			
Close	C			

Office 365 Account Profile Manager

To access the hot key mode in the Office 365 Account Profile Manager interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **U** to activate the hot keys for buttons on the ribbon.

Function Name and Hot Key			
Create	O	Save	S
		Cancel	C
Edit	E	Save	S
		Cancel	C
Delete	D		
Close	X		

Agent Proxy Settings

To access the hot key mode in the Office 365 Account Profile Manager interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **W** to activate the hot keys for buttons on the ribbon.

Function Name and Hot Key			
Proxy Settings	PS	Save	O
		Cancel	B
Close	C		

Security Profile

To access the hot key mode in the Security Profile interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **C** to activate the hot keys for buttons on the ribbon.

Function Name and Hot Key			
Create	N	Save	O
		Cancel	C
Edit	ED	Save	O
		Cancel	C
Delete	D		
Import	I		
Export	EP		
Close	X		

Managed Account Profile

To access the hot key mode in the Security Profile interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **R** to activate the hot keys for buttons on the ribbon.

Function Name and Hot Key			
Create	N	Save	O
		Cancel	C
View Details	V	Edit	E
		Cancel	C
Edit	E	Save	O
		Cancel	C
Delete	D		
Close	X		

Solution Manager

To access the hot key mode in the Solution Manager interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **T** to activate the hot keys for buttons on the ribbon.

Function Name and Hot Key			
Install	I		
Deploy	D		
Retract	R		
Remove	M		
Solution Properties	S	Deploy	D
		Retract	R
		Back	B

Function Name and Hot Key	
Retrieve Version	V
Upgrade	U
Close	X

Storage Configuration

To access the hot key mode in the Storage Configuration interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface.

Function Name and Hot Key					
Dashboard	B				
Create	N	Physical Device	P	Save	O
				Cancel	B
		Logical Device	L	Save	O
				Cancel	B
		Storage Policy	S	Save	O
				Cancel	B
View Details	T	Edit	E	Save	O
				Cancel	B
		Test Status	T		
		Cancel	B		
Edit	E	Save	O		
		Test Status	T		
		Cancel	X		
Delete	D				
Refresh	R				
Close	X				

Index Manager

To access the hot key mode in the Index Manager interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **X** to activate the hot keys for buttons on the ribbon.

Function Name and Hot Key					
New Index Profile	N	Save	S		
		Cancel	C		
View Details	VD	Edit	E	Save	S
				Cancel	C
		Cancel	C		
Edit	E	Save	S		
		Cancel	C		
Delete	D				

Function Name and Hot Key			
Configure Workday	CW	Save	S
		Cancel	C
Job Monitor	J		
Close	X		

Export Location

To access the hot key mode in the Export Location interface, use the key combination of **Ctrl** +**Alt** + **Z** on the keyboard, press **P** to go to the Control Panel interface, or press **E** to activate the hot keys for buttons on the ribbon.

Function Name and Hot Key					
Create	N	Save	S		
		Cancel	C		
View Details	V	Edit	E	Save	S
				Cancel	C
		Cancel	C		
Edit	E	Save	S		
		Cancel	C		
Delete	D				
Close	X				

Filter Policy

To access the Hot Key mode, in the Filter Policy interface, press the key combination of **Ctrl** +**Alt** + **Z** on the keyboard, press **P** to go to the Control Panel interface, or press **F** to activate the Hot Key of the buttons on the ribbon.

Function Name and Hot Key					
Create	N	Save	S		
		Cancel	C		
View Detail	N/A	Edit	E	Save	S
				Cancel	C
		Cancel	C		
Edit	E	Save	S		
		Cancel	C		
Delete	D				
Close	X				

Host Profile

To access the Hot Key mode in the Host Profile interface, press the key combination of **Ctrl** +**Alt** + **Z** on the keyboard, press **P** to go to the Control Panel interface, or press **HP** to activate the Hot Key of the buttons on the ribbon.

Function Name and Hot Key						
Create	C	Save	O			
		Cancel	X			
View Detail	V	Edit	E	Save	O	
				Cancel	X	
		Cancel	X			
Edit	E	Save	O			
		Cancel	X			
Delete	D					
Close	X					

Mapping Manager

To access the hot key mode in the Mapping Manager interface, press the **Ctrl** + **Alt** + **Z** key combination on your keyboard, press **P** to go to the Control Panel interface, or press **I** to activate the hot keys for buttons on the ribbon.

Function name and Hot Key							
Domain Mapping	D	Create	N	Import	I		
				Export	E		
				Save	S		
				Cancel	B		
		View Details	V	Export	p		
				Edit	E	Import	I
						Export	E
						Save	S
						Save As	A
						Cancel	B
				Cancel	B		
		Edit	E	Import	I		
				Export	E		
				Save	S		
				Save As	A		
				Cancel	B		
		Delete	R				
		Export	P				
		Close	X				
User Mapping	U	Create	N	Import	I		
				Export	E		
				Save	S		
				Cancel	B		
		View Details	V	Export	p		
				Edit	E	Import	I
						Export	E

Function name and Hot Key							
						Save	S
						Save As	A
						Cancel	B
				Cancel	B		
		Edit	E	Import	I		
				Export	E		
				Save	S		
				Save As	A		
				Cancel	B		
		Delete	R				
		Export	P				
		Close	X				
Language Mapping	L	Create	N	Import	I		
				Export	E		
				Save	S		
				Cancel	B		
		View Details	V	Export	p		
				Edit	E	Import	I
						Export	E
						Save	S
						Save As	A
						Cancel	B
				Cancel	B		
		Edit	E	Import	I		
				Export	E		
				Save	S		
				Save As	A		
				Cancel	B		
		Delete	R				
		Export	P				
		Close	X				
Column Mapping	N	Create	N	Import	I		
				Export	E		
				Save	S		
				Cancel	B		
		View Details	V	Export	p		
				Edit	E	Import	I
						Export	E
						Save	S
						Save As	A
						Cancel	B
				Cancel	B		
		Edit	E	Import	I		
				Export	E		
				Save	S		

Function name and Hot Key								
				Save As	A			
				Cancel	B			
		Delete	R					
		Export	P					
		Close	X					
Content Type Mapping	O	Create	N	Import	I			
				Export	E			
				Save	S			
				Cancel	B			
		View Details	V	Export	p			
				Edit	E	Import	I	
						Export	E	
						Save	S	
						Save As	A	
						Cancel	B	
				Cancel	B			
		Edit	E	Import	I			
				Export	E			
				Save	S			
				Save As	A			
				Cancel	B			
		Delete	R					
		Export	P					
		Close	X					
Template Mapping	T	Create	N	Import	I			
				Export	E			
				Save	S			
				Cancel	B			
		View Details	V	Export	p			
				Edit	E	Import	I	
						Export	E	
						Save	S	
						Save As	A	
						Cancel	B	
				Cancel	B			
		Edit	E	Import	I			
				Export	E			
				Save	S			
				Save As	A			
				Cancel	B			
		Delete	R					
		Export	P					
		Close	X					
Group Mapping	G	Create	N	Import	I			
				Export	E			

Function name and Hot Key								
				Save	S			
				Cancel	B			
		View Details	V	Export	p			
				Edit	E	Import	I	
						Export	E	
						Save	S	
						Save As	A	
						Cancel	B	
				Cancel	B			
		Edit	E	Import	I			
				Export	E			
				Save	S			
				Save As	A			
				Cancel	B			
		Delete	R					
		Export	P					
		Close	X					
List Name Mapping	LT	Create	N	Import	I			
				Export	E			
				Save	S			
				Cancel	B			
		View Details	V	Export	P			
				Edit	E	Import	I	
						Export	E	
						Save	S	
						Save As	A	
						Cancel	B	
				Cancel	B			
		Edit	E	Import	I			
				Export	E			
				Save	S			
				Save As	A			
				Cancel	B			
		Delete	R					
		Export	P					
		Close	X					

Using Hot Keys Mode in Plan Group

In order to work faster and improve your productivity, DocAve supports the hot key mode for you to perform corresponding actions quickly by only using your keyboard.

To access the hot key mode, press the **Ctrl** +**Alt** + **Z** key combination simultaneously on your keyboard while in the DocAve interface. Then press **5** to access the Plan Group.

The following sections provide lists of hot keys for the top level. Each time you want to go back to the top level after accessing the interface of lower level, press **Ctrl** + **Alt** + **Z** on the keyboard.

The following is a list of hot keys for Plan Group.

<table>
<tr><th colspan="10">Function Name and Hot Key</th></tr>
<tr><td rowspan="5">Create</td><td rowspan="5">N</td><td>Back</td><td colspan="7">B</td></tr>
<tr><td>Next</td><td colspan="7">N</td></tr>
<tr><td rowspan="2">Finish</td><td rowspan="2">F</td><td>Finish</td><td colspan="5">F</td></tr>
<tr><td>Finish and Run Now</td><td colspan="5">R</td></tr>
<tr><td>Cancel</td><td colspan="7">C</td></tr>
<tr><td rowspan="11">View Details</td><td rowspan="11">V</td><td>Plan Viewer</td><td colspan="7">P</td></tr>
<tr><td>Group Settings</td><td colspan="7">G</td></tr>
<tr><td rowspan="9">Edit</td><td rowspan="9">E</td><td>Add Plan(s)</td><td colspan="5">A</td></tr>
<tr><td>View Details</td><td colspan="5">V</td></tr>
<tr><td>Edit</td><td colspan="5">E</td></tr>
<tr><td>Remove</td><td colspan="5">R</td></tr>
<tr><td>Refresh</td><td colspan="5">RF</td></tr>
<tr><td rowspan="2">Save</td><td rowspan="2">S</td><td>Save</td><td>S</td></tr>
<tr><td>Save and Run Now</td><td>R</td></tr>
<tr><td>Cancel</td><td colspan="5">C</td></tr>
<tr><td>Cancel</td><td colspan="7">C</td></tr>
<tr><td rowspan="8">Edit</td><td rowspan="8">E</td><td>Add Plan(s)</td><td colspan="7">A</td></tr>
<tr><td>View Details</td><td colspan="7">V</td></tr>
<tr><td>Edit</td><td colspan="7">E</td></tr>
<tr><td>Remove</td><td colspan="7">R</td></tr>
<tr><td>Refresh</td><td colspan="7">RF</td></tr>
<tr><td rowspan="2">Save</td><td rowspan="2">S</td><td>Save</td><td>S</td></tr>
<tr><td>Save and Run Now</td><td>R</td></tr>
<tr><td>Cancel</td><td colspan="7">C</td></tr>
<tr><td>Delete</td><td colspan="9">D</td></tr>
<tr><td>Run Now</td><td colspan="9">R</td></tr>
<tr><td>Job Monitor</td><td colspan="9">J</td></tr>
</table>

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 © 2012-2015 AvePoint, Inc. All rights reserved. All materials contained in this publication are protected by United States and international copyright laws and no part of this publication may be reproduced, modified, displayed, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of AvePoint, 3 Second Street, Jersey City, NJ 07311, USA or, in the case of materials in this publication owned by third parties, without such third party's consent. Notwithstanding the foregoing, to the extent any AvePoint material in this publication is reproduced or modified in any way (including derivative works and transformative works), by you or on your behalf, then such reproduced or modified materials shall be automatically assigned to AvePoint without any further act and you agree on behalf of yourself and your successors, assigns, heirs, beneficiaries, and executors, to promptly do all things and sign all documents to confirm the transfer of such reproduced or modified materials to AvePoint.

Trademarks
AvePoint®, DocAve®, the AvePoint logo, and the AvePoint Pyramid logo are registered trademarks of AvePoint, Inc. with the United States Patent and Trademark Office. These registered trademarks, along with all other trademarks of AvePoint used in this publication are the exclusive property of AvePoint and may not be used without prior written consent.

Microsoft, MS-DOS, Internet Explorer, Office, Office 365, SharePoint, Windows PowerShell, SQL Server, Outlook, Windows Server, Active Directory, and Dynamics CRM 2013 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe Acrobat and Acrobat Reader are trademarks of Adobe Systems, Inc.

All other trademarks contained in this publication are the property of their respective owners and may not be used without such party's consent.

Changes
The material in this publication is for information purposes only and is subject to change without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, AvePoint makes no representation or warranty, expressed or implied, as to its completeness, accuracy, or suitability, and assumes no liability resulting from errors or omissions in this publication or from the use of the information contained herein. AvePoint reserves the right to make changes in the Graphical User Interface of the AvePoint software without reservation and without notification to its users.

AvePoint, Inc.
Harborside Financial Center, Plaza 10
3 Second Street, 9th Floor
Jersey City, New Jersey 07311
USA