DocAve® 6 Installation

User Guide

Service Pack 4, Cumulative Update 1

Revision T

Issued June 2016

Table of Contents

About the Installation Guide 6

Submitting Documentation Feedback to AvePoint 7

Before You Begin 8

SharePoint Agent Account Permissions 8

Reasons for Agent Account Permissions 9

Local Permissions 9

SQL Permissions 10

SharePoint Permissions 10

Adding DocAve 6 to Your Anti-Virus Exclusion List 11

Ports Used by DocAve 6 11

DocAve Manager System Requirements 18

System Requirements for Control Service Installation 19

System Requirements for Media Service Installation 22

System Requirements for Report Service Installation 22

DocAve Agent System Requirements 23

System Requirements for Agent Service Installation 23

SQL Server Requirements for DocAve Databases 24

SharePoint Environment Requirements for DocAve Agents 24

Overview of DocAve Manager Services and DocAve Agent Service 24

Configuring a Healthy DocAve Environment 25

Compatibility Matrix of DocAve and Governance Automation Versions 26

Installing DocAve 6 27

Installing DocAve Manager 27

Installing DocAve Manager on Common Environments 27

Installing DocAve Manager on Windows Server Core Environments 35

DocAve Control Service Load Balancing 36

Installing DocAve Agent 36

Installing DocAve Agent on Common Environments 37

Installing DocAve Agent on Windows Server Core Environments 39

Skipping Environment Scanning 40
Skipping Environment Scanning for DocAve Manager 40
Skipping Environment Scanning for DocAve Agent 40
Unattended Installation of DocAve Manager 41
Generating the Installation Answer File for DocAve Manager 41
Import the UnattendedInstallation.dll File 46
Commands and Command Parameters for DocAve Manager Unattended Installation 47
Getting Help Information About DocAve Manager Unattended Installation Commands 66
Unattended Installation of DocAve Agent 66
Generating the Installation Answer File for DocAve Agent 66
Import the UnattendedInstallation.dll File 68
Commands and Command Parameters for DocAve Agent Unattended Installation 69
Getting Help Information About DocAve Agent Unattended Installation Commands 81
Helpful Notes for DocAve Unattended Installation to Windows XP Operating System 82
Accessing the DocAve GUI 83
Internet Explorer Setup 83
Logging into DocAve 85
Out-of-Browser Accessing DocAve Manager 86
DocAve Manager and Agent Maintenance 88
Using the DocAve Manager/Agent Configuration Tool 88
Using the DocAve Manager/Agent Restart Service Tool 88
Using the DocAve Manager/Agent Uninstallation Wizard 88
Change the Manager Installation 89
Repair the Manager/Agent Installation 89
Uninstalling DocAve 90
Uninstalling DocAve Software 90
Storage Manager 90
Archiver 90
Connector 90
Uninstalling DocAve Manager 91
Uninstalling DocAve Manager from Common Environments 91
Uninstalling DocAve Manager from Windows Server Core Environments 92

Uninstalling DocAve Agent 93
Uninstalling DocAve Agent from Common Environments 93
Uninstalling DocAve Agent from Windows Server Core Environments 94
Advanced Configuration 95
Modify the Port Used by DocAve Storage Manager and Connector 95
Modify the Port Used by DocAve Replicator 95
Helpful Notes 97
Installed DocAve Agents Cannot be Displayed in the Manager Interface 97
Database Collation Issue 98
Other Issues 99
Appendix A: Where to Install DocAve Agents 100
Appendix B: Accessing Hot Key Mode 107
DocAve Home Page 107
Appendix C: Migration Source Environment 109
Appendix D: Permission Requirements for DocAve Modules 112
Migrator 112
File System Migrator 112
SharePoint Migrator 114
Lotus Notes Migrator 119
eRoom Migrator 121
Livelink Migrator 124
Exchange Public Folder Migrator 126
EMC Documentum Migrator 128
Quickr Migrator 130
Local System Permissions 133
Data Protection 133
Granular Backup and Restore 133
Platform Backup and Restore 136
SQL Server Data Manger 140
High Availability 141
Administration 145
Administrator 146

Content Manager 148
Deployment Manager 150
Replicator 152
Compliance 156
eDiscovery 156
Vault 157
Report Center 158
Local System Permissions 160
Storage Optimization 161
Storage Manager 161
Connector 162
Archiver 164
Notices and Copyright Information 167

About the Installation Guide

The DocAve 6 Installation Guide will provide you the following information:

- Order of installation
- System Requirements (minimum standards to proceed with the installation)
- System Recommendations (recommended standards for improved performance)

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

On a server running Windows Server 2003, before you install DocAve Manager using the Built-in database, Windows Installer 4.5 must be installed first. Download and install Windows Installer 4.5 prior to installing DocAve 6 Manager.

The 32-bit operating systems are not supported to use the built-in database when installing DocAve.

If you want to use the DocAve functions in SharePoint Online 2013, you must install .Net Framework 4.5 or the later versions on at least one of the Agent servers in the Agent Group used to perform the corresponding job.

SharePoint Agent Account Permissions

Ensure the SharePoint Agent account specified for DocAve 6 Agent has the following permissions:

1. Local System Permissions: The specified Agent Account will be granted Full Control permission to the following groups and folders during DocAve Agent installation:
    - IIS_WPG (for IIS 6) or IIS_IUSRS (for IIS 7 and IIS 8)
    - Performance Monitor Users
    - DocAve Users (the group is created by DocAve automatically and it has the following permissions):
        - Full Control to the Registry of HKEY_LOCAL_MACHINE\SOFTWARE\AvePoint\DocAve6.
        - Full Control to the Registry of HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\eventlog.
        - Full Control to the Communication Certificate.
        - Permission of **Log on as a batch job** (it can be found within Control Panel\Administrative Tools\Local Security Policy\Security Settings\Local Policies\User Rights Assignment)
        - Full Control Permission of DocAve Agent installation directory
        - Full Control Permission to the **Temporary Buffer**, which is configured in **Control Panel** > **Agent Monitor** > **Configure**
2. SharePoint Permissions:
    - Member of the **Farm Administrators** group
    - Permission to all zones of all of the Web applications via **User Policy for Web Application**
        - **Full Control** permission to all zones of all of the Web applications via **User Policy for Web Applications** in SharePoint 2010

        - **Full Control** and **Account operates as System** permission to all zones of all of the Web applications via **User Policy for Web Applications** in SharePoint 2013
    - User Profile Service Application permissions:
        - User Profile Service Application permissions in SharePoint 2010
            - Use Personal Features
            - Create Personal Site
            - Use Social Features
        - User Profile Service Application permissions in SharePoint 2013
            - Create Personal Site
            - Follow People and Edit Profile
            - Use Tags and Notes
    - Managed Metadata Service: Term Store Administrator
    - Business Data Connectivity Service: Full Control
    - Search Service: Full Control
3. SQL Server Permissions:
    - Database Role of **db_owner** in all the databases related with SharePoint, including content databases, SharePoint configuration database and Central Admin database.
    - Server Role of **dbcreator** and **securityadmin** in SQL Server.

Reasons for Agent Account Permissions

The DocAve 6 Agent Account permissions can be divided into three parts: Local, SQL, and SharePoint.

Local Permissions

The Agent Account should be added to the following three groups:

DocAve Users

DocAve requires particular permissions spread across the whole system, so DocAve creates the local group **DocAve Users** to account for these permissions. Then, admins can simply add users to this group to acquire the required permission.

Detailed Permissions for DocAve Users:

- Local Machine\Software\AvePoint\DocAve6 is created by DocAve installation.
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog: Permission to this registry is needed for writing to the event log.

- **Log on as a batch job** permission is used when DocAve starts a new process under the Agent account. DocAve uses batch log on and impersonate to create the new process.
- Full Control Permission to the **Temporary Buffer** is required when validating the Agent account's permission to the **Temporary Buffer** when changing the Agent account.

IIS_IUSRS (for IIS7 or 8) / IIS_WPG (for IIS6)

DocAve uses the WCF port sharing service; these groups have permissions to use port sharing.

Backup Operators

VSS backup needs this permission, but it can be ignored if you are not using Platform Backup & Restore.

Performance Monitor Users

DocAve uses .NET performance counter API, and SharePoint API also uses it internally. This permission is required by .NET API.

SQL Permissions

The Agent Account is required to act as the **db_owner** in all databases related to SharePoint, including Content Database, Config Database and Central Admin Database. This is because the SharePoint API operates these databases internally and therefore requires these permissions.

SharePoint Permissions

The Agent Account is required to be the **SharePoint Farm Administrator**. This is because DocAve need permission to browse Web applications, access farm services, etc.

The Agent Account is granted **Full Control Permission** to all zones of all Web applications via User Policy for Web Applications. DocAve needs this permission to access all site collections with the Agent Account. With **Full Control Permission**, the user is able to retrieve data such as Web template schema, field schema, and feature definition from 14 Hive via SharePoint API (even if UAC is enabled).

***Note**: For SharePoint 2013, the Agent Account is granted the Full control and **account operates as system account** to all zones of all Web applications via User Policy for Web Applications. **Account operates as system account** is needed to create the Microfeed list.

User Profile Service 2010

- **Use Personal Features**
  DocAve needs this permission to access user profile and user profile properties.
- **Create Personal Site**
  DocAve needs this permission to create personal site if needed.
- **Use Social Features**, which is related to Document Tagging, Social Comment (Document Notes)
  DocAve needs this permission to access and create social components, such as tags.

User Profile Service 2013

- **Create Personal Site**
  DocAve requires this for personal storage, newsfeed, and followed content.
- **Follow People and Edit Profile**
- **Use Tags and Notes**

Managed Metadata Service

- **Term Store Administrator**
  DocAve needs this permission to access and create term or keywords.

Business Data Connectivity Service

- **Full Control**
  This allows DocAve to get the schema of external content type.

Search Service

- **Full Control**
  DocAve needs this permission to access search scope and keywords.

Adding DocAve 6 to Your Anti-Virus Exclusion List

In some cases, your anti-virus software may negatively impact the performance of certain DocAve jobs. If you notice slow data transfer rates, or if you simply want to remove your anti-virus software from the job performance equation altogether, add the …*AvePoint**DocAve6* directory to your anti-virus software's exclusion list. This directory is the parent directory for all DocAve 6 executable files.

Ports Used by DocAve 6

Refer to the table below for the ports that are used by DocAve 6.

Port	Usage	Must be Enabled On …
14000	Website Port – Used to access DocAve Control service. Control Service Port – Used for communicating with other DocAve services.	DocAve Control Server
14001	Media Service Port – Used for communicating with other DocAve services.	DocAve Media Server
14002	Media Service Data Port – Used for transmitting data between DocAve and the storage device.	DocAve Media Server
14003	Report Service Port – Used for communicating with other DocAve services.	DocAve Report Server
14004	DocAve Agent Port – Used for communicating with other DocAve services.	DocAve Agent Server
14005	Port used by DocAve Storage Manager and Connector processes to transmit the data required by the enabled EBS/RBS provider.	N/A

Port	Usage	Must be Enabled On …
14006	Port used by DocAve Real-time Replicator to inform Replicator processes of the real-time actions captured in SharePoint.	N/A
14007	The proxy port to use when updating DocAve Control service by applying DocAve 6 updates in Update Manager.	DocAve Control Server
14009	Port used by DocAve Publishing Mode Replicator to transfer the data generated by publishing mode replication.	N/A
14100	Port used by eRoom Migration Tool to communicate with the main process of DocAve Migrator Tool	N/A

Refer to the table below for the ports that are used by each of the DocAve 6 products.

Product	Used Ports	Related Processes	Usage	Basic Functions Involved
Control Service Installation	14000	ControlTimerService.exe	Communicate with other services.	Install Control service.
Media Service Installation	14001 and 14002	MediaService.exe	Communicate with Control service and used for data transferring.	Install Media service and register it to the Control service.
Report Service Installation	14003	ReportService.exe	Communicate with other services.	Install Report service and register it to the Control service.
Agent Service Installation	14004	AgentService.exe	Communicate with Control service.	Install agent and register it to the Control service.
Control Panel	14007	CommonPatchInstaller.exe	PatchControlCli.exe process uses this port to communicate with the CommonPatchInstaller.exe processes of other services.	Update all the Manager/Agent services.

Product	Used Ports	Usage	Basic Functions Involved
SharePoint 2007 to 2010 Migration	14000	Communicate between Control service, Agent service and Media service.	Online migration at site collection level; Offline migration at site level.
	14001(Only for Offline Migration)	Communicate between Control service, Agent service and Media service.	Offline migrate site collection level.

Product	Used Ports	Usage	Basic Functions Involved
	14002(Only for Offline Migration)	Communicate between Control service, Agent service and Media service.	Offline migration at site collection level.
	14004	Communicate between Control service, Agent service and Media service.	Online migration at site collection level; Offline migration at site level.

Product	Used Ports	Related Processes	Usage	Basic Functions Involved
Report Center	14000 (Control service)	ControlTimerService.exe	Communicate between Control service, Agent service and Media service.	N/A
	14001 (Media service)	MediaService.exe	Communicate between Control service, Agent service and Media service.	Disk Space Monitoring
	14004 (Agent service)	SP2010ReportCenter.exe SP2010RCAuditor.exe	Communicate between Control service, Agent service and Report service.	Collect data; Run report; Show report; Apply Auditor rules; Retrieve Auditor data.
	14003 (Report service)	ReportService.exe	Communicate between Control service, Agent service and Report service.	

Product	Used Ports	Usage	Basic Functions Involved
Connector	14000	Communicate between Control service and Agent service.	Synchronization; Scheduled Synchronization; Mapping; Access Connector stubs.
	14004	Communicate between Control service and Agent service.	Synchronization; Scheduled Synchronization; Mapping; Access Connector stubs.
	14005	It is an internal port of the Connector process. Connector works well even if we don't create any Inbound Rule for this port.	Synchronization; Scheduled Synchronization; Mapping; Access Connector stubs.

Product	Used Ports	Related Processes	Usage	Basic Functions Involved
Granular Backup and Restore	14000	ControlTimerService.exe	Communicate between Control service, Agent service and Media service.	N/A

Product	Used Ports	Related Processes	Usage	Basic Functions Involved
	14001	MediaService.exe	Communicate between Control service, Agent service and Media service.	Granular backup; Granular restore.
	14004	SP2010GranularBackup.exe SP2010GranularRestore.exe	Communicate between Control service, Agent service and Media service.	Granular backup; Granular restore.

Product	Used Ports	Usage	Basic Functions Involved
Deployment Manager	14000	Communicate between Control service and Agent service.	Online Deployment Manager jobs; Offline Deployment Manager jobs.
	14001	Communicate between Control service, Agent service and Media service.	Deployment Manager jobs that checked the Backup the destination environment checkbox; Solution Store.
	14002	Transfer data between Media service and Agent service.	Deployment Manager jobs that checked the Backup the destination environment checkbox; Solution Store.
	14004	Communicate between Control service and Agent service.	Online Deployment Manager jobs; Offline Deployment Manager jobs.

Product	Used Ports	Usage	Basic Functions Involved
Content Manager	14000	Communicate with the Control service.	Create a Content Manager plan and run it.
	14001/ 14002	Communicate with the Media service.	Run a Content Manager job with the Backup the destination environment option selected and then roll back the source and destination.
	14004	Communicate with the Agent service.	Run a Content Manager job.

Product	Used Ports	Related Processes	Usage	Basic Functions Involved
Replicator	14000 (Control service)	ControlTimerService.exe	Communicate between Control service and Agent service.	Online Replicator job; Offline Replicator job; One-way Pull; Real-Time Replicator job.
	14004 (Agent service)	SP2010ReplicatorOffline.exe		
		SP2010ReplicatorPrimary.exe		
		SP2010ReplicatorSecondary.exe		
		SP2010ReplicatorListener.exe		
		SP2010GranularBackup.exe		

Product	Used Ports	Related Processes	Usage	Basic Functions Involved
		SP2013ReplicatorOffline.exe		
		SP2013ReplicatorPrimary.exe		
		SP2013ReplicatorSecondary.exe		
		SP2013ReplicatorListener.exe		
		SP2013GranularBackup.exe		
	14002 (Media service)	MediaService.exe	Communicate between Control service, Agent service and Media service.	Run a Replicator job with the Backup Before Replication option enabled.
	14006 (Agent service)	SP2010ReplicatorListener.exe	Replicator event handler uses this port to send event message to Replicator Listener process.	Real-Time Replicator job.
		SP2013ReplicatorListener.exe		
	14009 (Agent service)	SP2010ReplicatorWorker.exe	Use this port to transfer the data generated by publishing mode replication.	Publishing mode Replicator job.
		SP2013ReplicatorWorker.exe		

Product	Used Ports	Usage	Basic Functions Involved
Archiver	14000	Communicate between Control service, Agent service and Media service.	Archiver job; Archiver Restore job.
	14001		
	14002		
	14004		

Product	Used Ports	Usage	Basic Functions Involved
Exchange Public Folder Migration	14000 and 14004	Communicate between Manager and Agent.	Migrate source data to SharePoint using online migration.
eRoom Migration	14000 and 14004	Communicate between Manager and Agent.	Migrate source data to SharePoint using online migration; Migrate source data to SharePoint using offline migration.
	14100	Communicate between AgentToolEMMultiplePro	eRoom Migration Tool

Product	Used Ports	Usage	Basic Functions Involved
		cessesHelper.exe and MigratorTool.exe	
Livelink Migration	14000 and 14004	Communicate between Manager and Agent.	Migrate source data to SharePoint using online migration; Migrate source data to SharePoint using offline migration.
File System Migration	14000 and 14004		Migrate source data to SharePoint using online migration.
Lotus Notes Migration	14000 and 14004		Migrate source data to SharePoint using online migration; Migrate source data to SharePoint using offline migration.
EMC Documentation Migration	14000 and 14004		Migrate source data to SharePoint using online migration.
Quickr Migration	14000 and 14004		Migrate source data to SharePoint using online migration.

Product	Used Ports	Usage	Basic Functions Involved
Storage Manager	14000	Communicate between Control service and Agent service.	Apply Real-time Storage Manager rules; Apply Scheduled Storage Manager rules; Access Storage Manager stubs; Convert stubs to content; Clean up orphan BLOBs.
	14004	Communicate between Control service and Agent service.	Apply Real-time Storage Manager rules; Apply Scheduled Storage Manager rules; Access Storage Manager stubs; Convert stubs to content; Clean up orphan BLOBs.

Product	Used Ports	Usage	Basic Functions Involved
Administrator	14000	Communicate between Control service and Agent service.	Grant permission; Create site collections.
	14004	Communicate between Control service and Agent service.	Clone user permission; Dead account cleaner.

Except for the two local ports 14005 and 14006, all of the other ports must be able to be accessed through the firewall software installed on the corresponding machines.

***Note**: If there are multiple DocAve services installed on the same server, make sure all of the required ports are enabled on that server.

For example, if the **Windows Firewall** is enabled on the servers which have installed DocAve, you must make sure the 14000, 14001, 14002, 14003 and 14004 ports are allowed in the **Inbound Rules** on the corresponding servers.

***Note**: The port numbers may vary according to the settings configured when installing DocAve 6 in your environments. In this example, the default ports are used.

Remote to the server where the **DocAve 6 Timer Service** is installed, and complete the following steps:

1. Navigate to **Start** > **Administrative Tools** > **Windows Firewall with Advanced Security**.
2. Right click **Inbound Rules** under **Windows Firewall with Advanced Security on Local Computer** and click **New Rule**.
3. In **Rule Type** step, select **Port** to configure the inbound rule for the ports used by **DocAve 6 Timer Service**.
4. Click **Next**.
5. In **Protocol and Ports** step, specify the rule to be applied to **TCP**, and then select **Specific local ports** option. Enter 14000 in the textbox.
6. Click **Next**.
7. In **Action** step, select the **Allow the connection** option to allow the connection to the port 14000.
8. Click **Next**.
9. In **Profile** step, keep the default selection, which is selecting all the three options.
10. Click **Next**.
11. In **Name** step, enter the **Name** and an optional **Description** for this inbound rule.
12. Click **Finish** to finish creating the inbound rule.
13. Repeat the same steps on all the other servers which have DocAve installed and have enabled the **Windows Firewall**.

DocAve Manager System Requirements

DocAve Manager consists of three services, Control service, Media service, and Report service.

- Control service – Manage all DocAve operations and allows users to interact with the web-based DocAve platform. All agents can communicate with the manager through the Control service, so it is imperative that the machine you install the Control service on is accessible by all agent machines. This service can be run on a server cluster to achieve load balancing which leverages the Windows Network Load Balancer to automatically select the proper DocAve Control service for optimal performance. For more information, refer to the DocAve Control Service Load Balancing section of this guide.
- Media service – Performs assistant jobs such as managing the retention rules and managing the backup job data. This service can be installed on multiple machines. Using multiple media services allows for load-balanced access to the data storage locations.
- Report service – Manages all SharePoint data collection and management, monitor SharePoint activities and return the data to the Control service for processing. This must be configured with the associated SQL databases and SQL Report services. This service is critical for using the DocAve Report Center module.

  ***Note**: DocAve Report service can be installed on multiple servers and can be load balanced. However, all the Report services must share the same Report Database and Auditor Database.

They can either be run on the same server as your DocAve Agent, or split across several servers. For more information on DocAve Manager services, refer to Installing DocAve Manager.

While it is possible to have the DocAve Manager and DocAve Agent on a single server, it is not recommended. For the best performance, install the Manager's services across multiple servers, and install only the necessary Agents on the Agent servers.

Refer to these tables for the system requirements of each DocAve Manager Service:

- System Requirements for Control Service Installation
- System Requirements for Media Service Installation
- System Requirements for Report Service Installation

***Note:** If all Manager services are installed on the same server (or with a built-in database), all the system requirements mentioned in the System Requirements for Control Service Installation section must be met. Refer to the following table for the recommended configuration requirements to ensure your DocAve Manager can run smoothly.

Installation Scenarios	Processor	Available Physical Memory	Available Disk Space
Single Server with Control service, Media service, Report service	64-bit, 4 cores	4 GB	60 GB for system drive

Installation Scenarios	Processor	Available Physical Memory	Available Disk Space
Single Server with Control service, Media service, Report service using Built-in Database	64-bit, 4 cores	6 GB	80 GB for system drive

System Requirements for Control Service Installation

Rules		Requirements
Operating System Edition: **Windows Server 2008,** **Windows Server 2008 R2,** **Windows Server 2008 R2 SP1 Server Core,** **Windows 7,** **Windows 8,** **Windows Server 2012,** **Windows Server 2012 R2**	Number of CPU Cores	Recommended: 2 or greater
	Available Physical Memory	Required: 256 MB Recommended: 2 GB or greater
	Available Disk Space	Required: 1 GB
	.Net Framework Version	.NET Framework 3.5 SP1 or above (.NET Framework 3.5.1 must be installed)
	.Net Framework Features	For Windows Server 2008 SP2 and Windows Server 2008 R2 SP1: The Windows features, including WCF Activation, HTTP Activation and Non-HTTP Activation must be installed. For Windows Server 2012 and Windows Server 2012 R2: The Windows features, including .NET Framework 3.5.1, HTTP Activation, Non-HTTP Activation, WCF Services, and TCP Port Sharing must be installed.
	Net.Tcp Port Sharing Service	Net.Tcp Port Sharing Service is started
	Windows Process Activation Service	• Windows Process Activation Service is started • Process Model, .NET Environment and Configuration APIs are installed
	World Wide Web Publishing Service	World Wide Web Publishing Service is started

Rules		Requirements
	Web Server(IIS) Role	Windows features installed: • Web Server • Common HTTP Features (Static Content, Default Document) • For Windows Server 2008 SP2 and Windows Server 2008 R2 SP1: Application Development (ASP.NET, .NET Extensibility, ISAPI Extensions and ISAPI Filters) • For Windows Server 2012 and Windows Server 2012 R2: Application Development (ASP.NET 3.5, .NET Extensibility 3.5, ISAPI Extensions and ISAPI Filters) • Management Tools (IIS Management Console, IIS 6 Management Compatibility and IIS 6 Metabase Compatibility) ***Note**: IIS Management Console is not required to Windows Server 2008 R2 SP1 Server Core environment.
	IIS Admin Service	IIS Admin Service is started IIS version must be 6 or above
	PowerShell Version	PowerShell 2.0 or above
Operating System Edition: Windows Server 2003, Windows Server 2003 R2,	Number of CPU Cores	Recommended: 2 or greater
	Available Physical Memory	Required: 256 MB Recommended: 2 GB or greater
	Available Disk Space	Required: 1 GB
	.Net Framework Version	.NET Framework 3.5 SP1 or above (.NET Framework 3.5.1 must be installed)
	Net.Tcp Port Sharing Service	Net.Tcp Port Sharing Service is started
	World Wide Web Publishing Service	World Wide Web Publishing Service is started
	ASP.NET	ASP .Net 2.0.50727 or above

	Application Server	• Network COM+ access is enabled.
		• Internet Information Services (IIS) is started, including the following installed features:
		  ○ Common Files
		  ○ IIS Manager
		  ○ World Wide Web Service

Rules		Requirements
	IIS Service	IIS Admin Service is started IIS version must be 6 or above
	HTTP SSL	HTTP SSL Service is started
	PowerShell Version	PowerShell 2.0 or above

Required Application Pool Settings

The following application pool settings are required by DocAve Control Service Installation regardless if you choose to use an existing application pool or create a new one if you choose to:

- Create a new application pool; DocAve will automatically configure these settings.
- Use an existing application pool; you must configure the application pool according to the table below.

IIS Version	IIS Setting	Value	Note
IIS7	Advanced Settings > General > .NET Framework Version	v2.0 / v4.0	**No Managed Code** is not supported.
	Advanced Settings > General > Enable 32-bit Applications	False	**False** is required since DocAve must load some third-party dlls which are 64-bit ones.
	Advanced Settings > General > Managed Pipeline Mode	Integrated / Classic	It is not supported to use **Classic** together with **.NET Framework v4.0**.
	Process Model > Load User Profile	True	**True** is required by DocAve SSO, and **False** is not supported.
	Advanced Settings > General > Start Automatically	True / False	**True** is strongly recommended because if you set the value to **False**, the application pool requires manual starting up.

Required Application Pool Account Permissions

The application pool account for connecting an existing IIS website or creating a new IIS website must have the following **Local System Permissions**. The specified application pool account will be granted full control permission to the following groups and folders automatically during DocAve Manager installation.

The application pool account must be a member of the following local groups:

- IIS_WPG (for IIS 6) or IIS_IUSRS (for IIS 7 and IIS 8)
- Full Control to HKEY_LOCAL_MACHINE\SOFTWARE\AvePoint\DocAve6
- Full Control to DocAve Manager folder
- Member of the Performance Monitor Users group

- Full Control to DocAve Certificate private keys
- Full Control (or Read, Write, Modify and Delete) to C:\WINDOWS\Temp (only for Windows 2003 environment)

You can add the application pool account to the local **Administrators** group to meet the required permissions.

System Requirements for Media Service Installation

Rules		Requirements
Operating System Edition: **Windows Server 2003,** **Windows Server 2003 R2,** **Windows Server 2008,** **Windows Server 2008 R2,** **Windows Server 2008 R2 SP1 Server Core,** **Windows 7,** **Windows 8,** **Windows Server 2012,** **Windows Server 2012 R2**	Number of CPU Cores	Recommended: 2 or greater
	Available Physical Memory	Required: 128 MB Recommended: 1 GB or greater
	Available Disk Space	Required: 1 GB
	.NET Framework Version	.NET Framework 3.5 SP1 or above (.NET Framework 3.5.1 must be installed)
	.Net Framework 3.5 Features (only in **Windows Server 2008,** **Windows Server 2008 R2,** **Windows 7, Windows 8,Windows Server 2012, and Windows Server 2012 R2** environments)	For Windows Server 2008 SP2 and Windows Server 2008 R2 SP1: The Windows features, including WCF Activation, HTTP Activation and Non-HTTP Activation are installed. For Windows Server 2012 and Windows Server 2012 R2: The Windows features, including .NET Framework 3.5.1, HTTP Activation, Non-HTTP Activation, WCF Services, and TCP Port Sharing must be installed.
	Net.Tcp Port Sharing Service	Net.Tcp Port Sharing Service is started
	PowerShell Version	PowerShell 2.0 or above

System Requirements for Report Service Installation

Rules		Requirements
Operating System Edition: **Windows Server 2003,** **Windows Server 2003 R2,** **Windows Server 2008,** **Windows Server 2008 R2,**	Number of CPU Cores	Recommended: 2 or greater
	Available Physical Memory	Required: 128 MB Recommended: 1 GB or greater
	Available Disk Space	Required: 1 GB
	.NET Framework Version	.NET Framework 3.5 SP1 or above (.NET Framework 3.5.1 must be installed)
	.Net Framework 3.5 Features (only in **Windows Server 2008,**	For Windows Server 2008 SP2 and Windows Server 2008 R2 SP1: The Windows features, including WCF

Rules		Requirements
Windows Server 2008 R2 SP1 Server Core, Windows 7, Windows 8, Windows Server 2012, Windows Server 2012 R2	**Windows Server 2008 R2, Windows 7, Windows 8, Windows Server 2012, and Windows Server 2012 R2** environments)	Activation, HTTP Activation and Non-HTTP Activation are installed. For Windows Server 2012 and Windows Server 2012 R2: The Windows features, including .NET Framework 3.5.1, HTTP Activation, Non-HTTP Activation, WCF Services, and TCP Port Sharing must be installed.
	Net.Tcp Port Sharing Service	Net.Tcp Port Sharing Service is started
	PowerShell Version	PowerShell 2.0 or above

DocAve Agent System Requirements

DocAve Agent has one service, DocAve Agent service. A DocAve agent communicates with SharePoint based on the commands it receives from the DocAve Manager's Control service. Multiple agent setups provide redundancy as well as scalability for large environments by allowing you to specify different accounts for different farms where multiple farms exist. The DocAve Agent can be installed on different machines according to the role of the machine, and the DocAve modules and functionalities you wish to use. For more information on where to install the DocAve Agents, refer to Appendix A: Where to Install DocAve Agent.

System Requirements for Agent Service Installation

Rules		Requirements
Operating System Edition: Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2008 R2 SP1 Server Core, Windows XP, Windows Vista, Windows 7, Windows 8, Windows Server 2012, Windows Server 2012 R2	Number of CPU Cores	Recommended: 2 or greater
	Available Physical Memory	Required: 256 MB Recommended: 2 GB or greater
	Available Disk Space	Required: 1 GB
	.NET Framework Version	.NET Framework 3.5 SP1 or above
	.Net Framework 3.5 Features (only in **Windows Server 2008, Windows Server 2008 R2, Windows 7, Windows 8, Windows Server 2012, and Windows Server 2012 R2** environments)	For Windows Server 2008 SP2 and Windows Server 2008 R2 SP1: Windows .NET Framework 3.5.1 must be installed. For Windows Server 2012 and Windows Server 2012 R2: The Windows features, including WCF Services and TCP Port Sharing must be installed.
	Net.Tcp Port Sharing Service	Net.Tcp Port Sharing Service is started
	PowerShell Version	PowerShell 2.0 or above

SQL Server Requirements for DocAve Databases

Databases	SQL Server Edition
Control Database	For DocAve 6 SP4 CU1 and the later versions: • Microsoft SQL Server 2005 • Microsoft SQL Server 2008 • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2012 • Microsoft SQL Azure • Microsoft SQL Server 2012 Business Intelligence • Microsoft SQL Server 2014
Report Database	
Auditor Database	
Replicator Database	
Stub Database	
Migrator Database	

SharePoint Environment Requirements for DocAve Agents

DocAve 6 Agents are compatible with the following SharePoint platforms:

- Microsoft SharePoint Server/Foundation 2010 (up to and including Service Pack 2)
- Microsoft SharePoint Server/Foundation 2013 (up to and including Service Pack 1)

***Note**: The all-in-one installation of SharePoint uses the Complete installation option, which installs everything (including SQL Server) on a single machine. If you are using the SharePoint Stand-alone installation that uses a built-in SQL Server 2008 Express database, Web applications using the pre-defined **Network Service** account as the application pool security account are not supported by DocAve 6 because local users may be used to manage certain SharePoint components.

Overview of DocAve Manager Services and DocAve Agent Service

After installing all of the services including DocAve Manager Services and DocAve Agent service properly, you are able to manage your SharePoint data via the DocAve platform.

Control service receives the request from DocAve Manager GUI, and then sends the request to Agent services which retrieve data from SharePoint. Agent services transfer the SharePoint data to Media services where the data will be integrated to the format only that can be identified by DocAve and send the integrated data to the specified destination. Agent services also retrieve data via Media service when transferring or restoring data to SharePoint. The Report service records all of these actions. The information is then used by DocAve when generating reports.

DocAve Control service and DocAve Agent service are required for all the DocAve products. DocAve Media service is required for all the following DocAve products:

- Granular Backup and Restore
- Platform Backup and Restore
- Archiver

- Deployment Manager
- Replicator
- Content Manager
- eDiscovery
- SharePoint 2007 to 2010 Migration

DocAve Report service is only required to DocAve Report Center product. You do not have to install DocAve Report service if you are not using DocAve Report Center.

Configuring a Healthy DocAve Environment

The following table lists the criteria for what constitutes a healthy DocAve environment:

Requirement	Reason	Mandatory?
Manager installed	Fundamental to update configurations	Yes
Agents installed on each DocAve 6 SP1 Agent host	Fundamental for all farms to be updated	Yes
Media service installed on each DocAve 6 SP1 media server	Fundamental for all farms to be updated	Yes
Manager sees Agents in Agent Monitor	Test of communication between Manager / Agents	Yes
Manager sees Media services in Manager Monitor	Test of communication between Manager / Media	Yes
Tree loads in all installed products	Test of communication and access rights between DocAve Agent account provided and SharePoint	Yes
Backup run against sample Web application	Test the configuration of VSS in the environment	Preferred
EBS or RBS is installed on each Agent	Verify EBS or RBS runtime is installed on each Agent	Preferred
RBS tested against sample content DB	Test of communication between Agents and the SharePoint environment	Preferred

Compatibility Matrix of DocAve and Governance Automation Versions

For a compatibility matrix of DocAve and Governance Automation versions, refer to the AvePoint KB article Compatibility Matrix of DocAve and Governance Automation.

Installing DocAve 6

The DocAve 6 Installation Wizards guide you through the installation process. By following the steps below, you will have DocAve up-and-running on your environment very quickly. To complete the installation successfully, a local administrator must be used to run the Installation Wizard.

To install DocAve 6, complete the steps below in order:

1. Installing DocAve Manager.
2. Installing DocAve Agent.

***Note**: After the Manager and Agent installation complete, you can log into DocAve to make sure the Manager and Agent are able to communicate with each other properly. To access the DocAve GUI, refer to Accessing the DocAve GUI.

***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. For more information on managing your DocAve license, refer to the **License Manager** section in the Control Panel Reference Guide.

Installing DocAve Manager

Before installing DocAve Manager, ensure that the DocAve Manager System Requirements are met on the servers where you want to install the DocAve Manager services.

The following sections describe the steps for installing DocAve Manager on common environments and Windows Server Core environments.

Installing DocAve Manager on Common Environments

DocAve Manager can be installed using the DocAve Manager Installation Wizard on the following environments.

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows 7
- Windows 8
- Windows Server 2012

- Windows Server 2012 R2

***Note**: When running the Manager Installation Wizard on the server running Windows Server 2003/Windows Server 2003 R2, make sure the Windows components are not being added or removed during the rule scanning, otherwise, the scanning result will be affected.

***Note**: When running the Manager Installation Wizard on a server running Windows Server 2008/Windows Server 2008 R2/Windows 7/Windows Server 2012/Windows Server 2012 R2, make sure the Server Manager is not being used to add or remove Windows features during the rule scanning; otherwise, the scanning result will be affected.

To install DocAve Manager, complete the following steps:

1. Download the Manager ZIP file, either by requesting a demo version or by contacting an AvePoint representative for links to this package.
2. Unzip this package. Open this unpacked DocAve Manager directory. Double click the *Setup.exe* file.
3. After the welcome screen appears, click **Next**.
4. Enter your name and the organization into the provided field. Click **Next**.
5. Carefully review the DocAve License Agreement. After you have read the agreement, check the **I accept the terms in the license agreement** checkbox, and click **Next**.

   ***Note**: After the Manager installation completes, you can navigate to the Manager installation path **…\DocAve6\Manager\lic** to check all the demo license agreements with different versions.
6. Click the **Browse** button. Select the location for the Manager installation. By default, the installation location is *C:\Program Files\AvePoint*. Click **Next**.
7. Select the DocAve Manager services you want to install. There are two installation methods you can select, **Complete** or **Advanced**.
   - **Complete** – All of the services will be installed onto one machine.
   - **Advanced** – Only the selected service will be installed. Select the services you want to install by checking the corresponding checkbox. There are three services you can install:
     - **Control Service** – Manage all DocAve operations and achieve the web-based DocAve platform, allowing users to interact with the software. All agents can communicate with the manager by Control service, so it is imperative that the machine you install the Control service on is accessible by all agent machines. This service can be run on a server cluster to achieve load balancing which leverages the Windows Network Load Balancer to automatically select the proper DocAve Control service for optimal performance. For more information, refer to the DocAve Control Service Load Balancing section of this guide.

- **Media Service** – Performs assistant jobs such as managing the retention rules and managing the backup job data. This service can be installed on multiple machines. Using multiple media services allows for load-balanced access to the data storage locations.
- **Report Service** – Manages all SharePoint data collection and management, monitor SharePoint activities and return the data to the Control service for processing. This must be configured with the associated SQL databases and SQL Report services. This service is critical for using the DocAve Report Center module.

  ***Note**: DocAve Report service can be installed on multiple servers and can be load balanced. However, all the Report services must share the same Report Database and Auditor Database.

Click **Next**.

8. DocAve will perform a brief pre-scan of the environment to ensure that all rules meet the requirements. The status for each rule will be listed in the **Status** column. Click the hyperlink of the status, the detailed information about the scan result will be listed in the popup window. You may click **Details** to can view the detailed information of all the requirements.

   If any rules have failed the pre-scan, update your environment to meet the requirements, then click the **Rescan** button to check your environment again. Once all rules pass, click **Next**.

9. Set up the Control Service Configuration:

   - **Control Service Host** – Specify the current machine's hostname, IP address, or fully qualified domain name (FQDN). The Control service manages internal configuration data, user access control, scheduling, and job monitoring.

     ***Note:** You must ensure that the Control service host can communicate with all of the Agent machines through the entered hostname, IP address, or FQDN.

   - **IIS Website Settings** – Configure the IIS website settings for the Control service. You can select to use an existing IIS website or create a new IIS website. The IIS website is used to access DocAve Manager.
     - **Use an existing IIS website** – Select an existing IIS website from the drop-down list, and if necessary, you can adjust the **Website Port** used to access the DocAve Control service.
     - **Create a new IIS website** – Enter the website name and create a new IIS website for the Control service. The default **Website Port** used to access DocAve Control service is 14000. You do not need to change it unless a known port conflict exists.
     - **Website Port** – Control service communication port. The default port is 14000.
   - **Application Pool Settings** – Configure the IIS application pool settings for the corresponding website. You can select to use an existing application pool or create a

new application pool. The application pool is used to handle the requests sent to the corresponding website.

The following settings can be configured:

- **Use an existing application pool** – Select an existing application pool from the drop-down list. If you choose to use an existing application pool, the Application Pool Account settings are greyed out and cannot be changed.
- **Create a new application pool** – Enter the application pool name and application pool account settings to create a new IIS application pool for the corresponding website.

Click **Next** to continue to configure the database settings for Control service.

10. Select **MS SQL** or **Built-in Database** from the Database Type drop-down menu to configure the database.

    - For the MS SQL database, the following information must be configured:
        - **Database Server** – The MS SQL server name.
        - **Control Database Name** – Enter a database name for the Control service, if the database does not exist, it will be created in the provided MS SQL server.
        - **Database Credentials** – Select the credential for this Control database.
            - **Windows Authentication** (the default option) – Use this method when you want the user identity to be confirmed by Windows. The account must have the following permissions.

              Local Permissions – The user must have the following permission to the machine where the DocAve Manager will be installed: Log on as a batch job (found in **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Security Settings** > **Local Policies** > **User Rights Assignment**).

              SQL Permissions – The user must have permission to access the SQL Server machine where you want to create the Control database. Also, the user must have the following permission: **db_owner** database role in the existing DocAve 6 Control database or **dbcreator** server role in the SQL Server that will contain the newly created DocAve 6 Control database.

            - **SQL Authentication** – SQL server will confirm the user identity itself according to the specified account and password. The specified account must have the following permission: **db_owner** database role in the existing DocAve 6 Control database or **dbcreator** server role in the SQL Server that will contain the newly created DocAve 6 Control database.
        - **Passphrase Settings** – This field is available if you choose to create a new Control database. Enter the passphrase for the Control database you are about

to create. The passphrase is used to protect the DocAve Manager data in the newly created Control database.

- If selecting the **Show Characters** option, the entered passphrase will be displayed in clear text, and it will be displayed on the **Complete** interface.
- If you are not selecting the **Show Characters** option, the entered passphrase will be displayed in encrypted text, and it will not be displayed on the **Complete** interface.

  ***Note**: If you choose to use an existing Control database, you will not be required enter the previously configured passphrase for the entered Control database in this page. You will be required to enter the previously configured passphrase for using this Control database in the **Passphrase Settings** page in the next step.

- If you choose to use the same Control database with the previously installed Control service on the current server, and the configuration file for the previously installed DocAve Manager on the current server has not been removed during the uninstallation, you can use this Control database without entering the previously configured passphrase.

- **Advanced Database Settings** – You can choose to associate the DocAve Control database with a specific failover SQL server that is used in conjunction with SQL Server database mirroring.

- For **Built-in Database**, enter the passphrase you want to use for protecting DocAve Manager data in the **Passphrase Settings** textbox.

***Note**: The built-in database only supports the all-in-one installation. After the Manager installation completes, it cannot be changed using the **Change** function.

Click **Next**.

11. If you choose to use an existing Control database in the previous step, the **Passphrase Settings** page appears. Enter the previously configured passphrase for the Control database you want to use in the **Passphrase** text box.

    ***Note**: I If you choose to use the same Control database with the previously installed Control service on the current server, and the configuration file for the previously installed DocAve Manager on the current server has not been removed during the uninstallation, you can use this Control database without entering the previously configured passphrase, and this page will not appear.

    - If you select the **Show Characters** option, the entered passphrase will be displayed in clear text, and it will be displayed on the **Complete** interface.
    - If you deselect selecting the **Show Characters** option, the entered passphrase will be displayed in encrypted text, and it will not be displayed on the **Complete** interface.

Click **Next**.

12. Set up the **Media Service Configuration** for data management.

    - **Media Service Host** – Specify the current machine's hostname or IP address. The Media service manages backup job data (for example, job metadata and backup index from Data Protection).
    - **Media Service Port** – Used for communicating with the other DocAve services. The default port is 14001.
    - **Media Service Data Port** – Transmit the data between DocAve and the storage device. The default port is 14002.
    - **Control Service Host** (This field will be hidden when you choose to install the Control Service in Services Installation step) – The hostname or IP address of the machine where Control service is installed.
    - **Control Service Port** (This field will be hidden when you choose to install the Control Service in Services Installation step) – The port number for the Control service entered above.

    ***Note**: The **Control Service Host** and **Control Service Port** must be consistent across all DocAve Manager Services in order to properly function.

    Click **Next**.

13. Set up the **Report Service Configuration**.

    - **Report Service Host** – The hostname or IP address of the machine where Report service is installed.
    - **Report Service Port** – The port number for Report service. The default port is 14003.
    - **Control Service Host** (This field will be hidden when you choose to install the **Control Service** in **Services Installation** step) – The hostname or IP address of the machine where Control service is installed.
    - **Control Service Port** (This field will be hidden when you choose to install the **Control Service** in **Services Installation** step) – The port number for the Control service entered above.

    ***Note**: The **Control Service Host** and **Control Service Port** must be consistent across all DocAve manager services in order to properly function.

    Click **Next** to continue to configure the database settings for Report service.

14. For the **Report Database Settings**, you can select to use the previous database settings or configure it yourself:

    - **Use the previous database settings** – If you select this option under Report service Configuration, the previous database settings for Control database will be used for the report database.

To set a database for report service only, the following information must be configured.

- Select the database type from the drop-down list, now only MS SQL can be selected.
    - **Database Server** – The MS SQL server name.
    - **Report Database Name** – Enter a database name for the Report service, if the database does not exist, it will be created in the provided MS SQL server.
    - **Database Credentials** – Select the credential for this Report database.
        - **Windows Authentication** (the default option) – Use this method when you want the user identity to be confirmed by Windows. . The account must have the following permissions.

          Local Permissions – The user must have the following permission to the machine where the DocAve Manager will be installed: Log on as a batch job (found in **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Security Settings** > **Local Policies** > **User Rights Assignment**).

          SQL Permissions – The user must have the permission of accessing the SQL Server machine where you want to create the report database. Also, the user must have the following permission: **db_owner** database role in the existing DocAve 6 Report database or **dbcreator** server role in the SQL Server that will contain the newly created DocAve 6 Report database.

        - **SQL Authentication** – SQL server will confirm the user identity itself according to the specified account and password. The specified account must have the following permission: **db_owner** database role in the existing DocAve 6 Report database or **dbcreator** server role in the SQL Server that will contain the newly created DocAve 6 Report database.
    - **Advanced Database Settings** – You can choose to associate the DocAve Report database with a specific failover SQL server that is used in conjunction with SQL Server database mirroring.

Click **Next** to continue to configure the Auditor database settings for Report service.

15. For the **Auditor Database Settings**, you can select to use the previous database settings or configure it by yourself.

    - **Use the previous database settings** – If you select this option, the previous database settings for the Report database will be used for the Auditor database.

    To set an auditor database for report service only, configure the following information:

    - Select the database type from the drop-down list, now only MS SQL can be selected.
        - **Database Server** – The MS SQL server name.

***Note**: It is recommended creating the DocAve Auditor database on a different SQL server other than the SQL server which stores the SharePoint databases.

If you put the DocAve Auditor database and SharePoint database on the same SQL Server, as the SharePoint Auditor data grows, large amount of disk space of the SQL Server machine will be occupied when DocAve Compliance Reports fetches data from SharePoint Auditor database and stores it to DocAve Auditor database. Thus the response of both SQL Server and SharePoint will become slow.

- **Auditor Database Name** – Enter a database name for the Auditor database, if the database does not exist, it will be created in the provided MS SQL server.
- **Database Credentials** – Select the credential for this Auditor database.
  - **Windows Authentication** (the default option) – Use this method when you want the user identity to be confirmed by Windows. The account must have the following permissions.

    Local Permissions – The user must have the following permission to the machine where the DocAve Manager will be installed: Log on as a batch job (found in **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Security Settings** > **Local Policies** > **User Rights Assignment**).

    SQL Permissions – The user must have the permission of accessing the SQL Server machine where you want to create the Auditor database. Also, the user must have the following permission: **db_owner** database role in the existing DocAve 6 Control database or **dbcreator** server role in the SQL Server that will contain the newly created DocAve 6 Control database.

  - **SQL Authentication**– SQL server will confirm the user identity itself according to the specified account and password. The specified account must have the following permission: **db_owner** database role in the existing DocAve 6 Auditor database or **dbcreator** server role in the SQL Server that will contain the newly created DocAve 6 Auditor database.
- **Advanced Database Settings** – You can choose to associate the DocAve Auditor database with a specific failover SQL server that is used in conjunction with SQL Server database mirroring.

Click **Next**.

16. In the **Advanced Configuration** page, specify the **SSL certificate** for encrypting the communication between the DocAve Manager and DocAve Agents.

    - **Build-in Certificate** – Uses the certificate provided by DocAve. No additional configuration is necessary.

- **User-defined Certificate** – Enabling this option allows you to select a certificate from your local machine. Use the Certificate Authentication server of the current machine to check whether the certificate is revoked and filter the certificates to only display the certificates that are not revoked.

Click **Next**.

17. In the **Ready to install DocAve Manager** page, the information of **Name**, **Organization**, **Services**, and **Database** configured in the previous steps is listed. Click **Install** to begin the installation. Click **Back** to change any of the previous settings. Click **Cancel** to abandon all configurations and exit the installation wizard.
18. When the Manager installation is completed, the Manager Passphrase you specified to protect DocAve Manager data will be displayed on the **Install Completed** page. Save this passphrase as you need to enter it for the agent installation.
19. Select the checkbox in front of **Register DocAve now to provide feedback on your platform and enhance AvePoint technical support** to enable the Customer Experience Improvement Program (CEIP) function. The CEIP function can help to improve technical support by sending DocAve usage feedback to AvePoint.
20. Click **Finish** to complete the installation and exit the installation wizard.

Installing DocAve Manager on Windows Server Core Environments

To install DocAve Manager on Windows Server 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core environment, complete the following steps:

1. Generate the Manager Installation Answer file on a server that does not use the Windows Server Core operating system.

   The Answer file is an XML file which provides configuration information required for DocAve Manager Installation on Windows Server 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core environments. Since the DocAve Setup Manager wizard which generates the Answer file cannot be run on Windows Server 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core environments, you must first run the DocAve Setup Manager on a Windows environment to generate the Answer file necessary for installing the DocAve Manager on a Windows Server 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core environment. Refer to the Generating the Installation Answer File for DocAve Manager section for more information.

2. Change the directory to the unzipped DocAve Manager installation package in the Command Line interface.

   Enter the Manager installation command with the Answer file path, and press **Enter** to start the DocAve Manager installation process. The command is:

Setup.exe Install-DocAveManager "c:\AnswerFileManager.xml"

3. The prompt message **Complete** is displayed in the Command Line interface when the Manager installation completes.

DocAve Control Service Load Balancing

DocAve Control Service Load Balancing can be achieved by installing DocAve Control services on multiple servers within the same Windows Network Load Balanced cluster using the same Control service database. After configuring the Load balancing, the Windows Network Load Balancer will handle the received request and send them to the optimal Control service.

Before using the DocAve Control Service Load Balancing, make sure the following requirements are met:

- Enter the hostname or IP address of each individual server when installing DocAve Control service on the corresponding server.
- Use the Network Load Balanced cluster public IP address when installing other DocAve Manager services.
- Use the Network Load Balanced cluster public IP address when installing DocAve Agents.
- Use the Network Load Balanced cluster hostname and public IP address when accessing DocAve.

***Note**: A **Report Location** must be configured in Job Monitor before you can use the Log Manager and Job Monitor when DocAve Control Service Load Balancing is used. Otherwise, each server where Control service is installed will retain its own log for just the jobs carried out by the control service installed on the server. For more information, refer to the DocAve 6 Job Monitor Reference Guide.

Installing DocAve Agent

Before installing DocAve Agent, ensure that the following requirements are met:

- The DocAve Agent System Requirements are met on the server where you want to install the Agent. For more information on where to install the DocAve Agents according to the products you wish to use, refer to Appendix A: Where to Install DocAve Agents.
- Ensure that the following services are started before installing the DocAve Agent:
    - The DocAve Manager Control service to which the DocAve Agent service will connect.
    - The Windows Management Instrumentation service on the server where you will install the Agent.

The following sections describe the steps for installing DocAve Agents on common environments and Windows Server Core environments.

Installing DocAve Agent on Common Environments

DocAve Agent is able to be installed using the DocAve Agent Installation Wizard on the following common Windows environments:

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows Server 2012
- Windows Server 2012 R2

After the DocAve Manager's Control service to which the Agent service will connect has been started, complete the following steps to install the DocAve Agent:

1. Download the Agent ZIP file, either by requesting a demo version or by contacting an AvePoint representative for links to this package.
2. Unzip this package and navigate to the DocAve Agent directory. Double click the *Setup.exe* file.
3. From the welcome screen, click **Next**.
4. Enter your name and organization into the provided fields, and click **Next**.
5. Carefully review the DocAve License Agreement, check the **I accept the terms in the license agreement** checkbox, and then click **Next**.

   ***Note**: After the Agent installation completes, you can navigate to the Agent installation path …*DocAve6**Agent**lic*\ to check all the demo license agreements with different versions.
6. Click the **Browse** button. Select the location for the Agent installation. By default, the installation location is: *C:**Program Files**AvePoint*. Click **Next**.
7. DocAve will perform a brief pre-scan of the environment to ensure that all rules meet the requirements. The status for each rule will be listed in the Status column. Click the hyperlink of the status, the detailed information about the scan result will be listed in the popup window.

   Click **Details** and you can view the detailed information of all the requirements.

Update your environment to meet the requirements if there are some rules checked failed. Click the **Rescan** button to check your environment again.

Once all rules pass, click **Next**.

8. Prior to setting up the **Communication Configuration** between the Agent host and the Control service host, you must ensure the following requirements are met:

    - The Control service has been installed on a specific machine which can communicate with the current server.
    - The current server's Internet Explorer browser is not using a proxy server.

    With the requirements above are met, set up the **Communication Configuration**:

    - **DocAve Agent Host** – Specify the current server's hostname, IP address or fully qualified domain name (FQDN).

      ***Note**: If the network connection of the current server is using the Internet Protocol Version 6 (TCP/IPv6) and you want to enter the IP address of the current server into the **DocAve Agent Host** text box, do not enter the link-local IPv6 address.

    - **DocAve Agent Port** – The port specified here is used by the Manager or other Agents for communication. The default port number is 14004.
    - **Control Service Host** – The hostname or IP address of the machine where the Control service is installed.
    - **Control Service Port** – This is the port used for communication with Control service and should match the information provided during the Manager configuration. The default port number is 14000.
    - **SSL Certificate** – Specify the SSL Certificate for encrypting the communication between this DocAve Agent and DocAve Manager.
        - **Build-in Certificate** – Uses the certificate provided by DocAve. No additional configuration is necessary.
        - **User-defined Certificate** – Enabling this option allows you to select a certificate from your local machine. Use the Certificate Authentication server of the current machine to check whether the certificate is revoked and filter the certificates to only display the certificates that are not revoked.

          ***Note**: To ensure that the DocAve Agent can communicate with the DocAve Manager properly, the DocAve Agent and Manager should use the same SSL certificate or different certificates issued by the same Certificate Authority.

    Click **Next**.

9. Set up the **Agent Configuration**:

- **Agent Authentication** – Specify the Manager Passphrase specified when configuring the DocAve Manager installation. If you forget the passphrase, you can view it by navigating to **DocAve** > **Control Panel** > **System Settings** > **System Options** > **Security Settings**. For more information, refer to the DocAve 6 Control Panel Reference Guide.
- **Agent Account** – Specify the Agent account under which the Agent activities are performed. For detailed information on the permissions required for each DocAve module, refer to that module's user guide. The ideal account permissions for all DocAve products are specified below.

Click **Next**.

10. In the **Ready to install DocAve Agent** Page, review the customer information you defined.
11. Click **Install** to begin the installation. Click **Back** to change any of the previous settings. Click **Cancel** to abandon all configurations and exit the installation wizard.
12. After the installation is completed, click **Finish** to exit the installation wizard.

Congratulations! DocAve is now installed and configured. Once you have completed the product installation, you can begin to configure logical and physical devices needed to store backup data.

Installing DocAve Agent on Windows Server Core Environments

Once the Manager's services have started, complete the following steps to install the DocAve Agent on Windows Server 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core environment:

1. Generate the Agent Installation Answer file on a server that does not use the Windows Server Core operating system.

   The Answer file is an XML file which provides configuration information required for DocAve Agent installation on Windows Server 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core environments. Since the DocAve Setup Manager wizard which generates the Answer file cannot be run on Windows Server 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core environments, you must first run the DocAve Setup Manager on a Windows environment to generate the Answer file necessary for installing the DocAve Agent on a Windows Server 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core environment. Refer to the Generating the Installation Answer File for DocAve Agent section for more information.

2. Change the directory to the unzipped DocAve Agent installation package in the Command Line interface.
3. Enter the Agent installation command with the Answer file path, and press **Enter** to start the DocAve Agent installation process. The command is: *Setup.exe Install-DocAveAgent "c:\AnswerFileAgent.xml"*.

4. The prompt message **Complete** is displayed in the Command Line interface when the Agent installation completes.

Skipping Environment Scanning

System requirements must be met in order for DocAve to work properly. If you are certain that you meet all of the system requirements are met, the following sections provide instructions on skipping environment scanning for DocAve Manager and Agent installation.

***Note**: Environment scanning cannot be skipped when installing DocAve on Windows Server 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core environment.

Skipping Environment Scanning for DocAve Manager

Follow the instructions below to skip environment scanning for DocAve Manager.

1. In the Command Line Interface, change the directory to the extracted DocAve Manager package where the **Setup.exe** file resides.
2. Enter the following command to skip environment scanning.
    - To skip system information scanning during DocAve Manager installation, enter the following command to launch the Manager installation program:

      Setup.exe -SkipRuleChecking

    - To skip SQL Server version scanning during DocAve Manager installation, enter the following command to launch the Manager installation program:

      Setup.exe -SkipSQLChecking

    - To skip both system information scanning and SQL Server version scanning during DocAve Manager installation, enter the following command to launch the Manager installation program:

      Setup.exe -SkipRuleChecking -SkipSQLChecking

2. The scan status of each requirement displays **Skip** in the **Installation Rule Scanning** step during Manager installation.

Skipping Environment Scanning for DocAve Agent

Follow the instructions below to skip environment scanning for DocAve Agent.

1. In the Command Line Interface, change the directory to the extracted DocAve Agent package where the **Setup.exe** file resides.
2. To skip system information scanning during DocAve Agent installation, enter the following command to launch the Agent installation program:

Setup.exe -SkipRuleChecking

3. The scan status of each requirement displays **Skip** in the **Installation Rule Scanning** step during Agent installation.

Unattended Installation of DocAve Manager

Make sure the system requirements are met before starting the DocAve Manager unattended installation. For more information, refer to DocAve Manager System Requirements.

Generating the Installation Answer File for DocAve Manager

The Answer file is an XML file which provides configuration information required for the unattended installation. Before performing the unattended installation, the Answer file must be generated using the DocAve 6 Setup Manager.

Navigate to the …*UnattendedInstall**SetupManager* folder inside the unzipped Manager installation package, and double click **SetupManager.exe** to run it. Complete the following steps:

1. After being presented with the welcome screen, click **Next**.
2. Select **Create a new answer file for DocAve 6 Manager** to create a new Answer file for DocAve Manager.
    - **Modify an existing answer file** – Select this option to reuse an existing Answer file. If this is selected, the path field will be enabled. Enter the full path of the answer file is or click **Browse** to browse for an answer file. For example, C:\AnswerFile.xml

      ***Note**: We recommend you create a generic Answer file so that it can be reused later with modification.

      Click **Next**.
3. Carefully review the DocAve License Agreement.

   After you have read the terms in the license agreement, check the **I accept the terms in the license agreement** checkbox to agree to the terms. Click **Next**.
4. Enter your name and the organization into the provided field. Click Next to continue the configuration. Click **Back** to return to the previous interface.
5. Set up the installation location using the following conditions.
    - **Default directory** – The DocAve Manager will be installed to the default installation location on the specified destination server, which is …*Program Files**AvePoint**DocAve6**Manager.*
    - **Customized directory** – If you select this option, enter a customized path in the **Installation Path** field where you wish to install the DocAve Manager on the destination server.

- **Use the default directory if your customized directory is invalid** – Enable this option to install DocAve Manager to the default directory should the path you defined for customized directory be invalid. For example, if the drive indicated by the path you specified does not exist on the destination server.

6. Select the DocAve Manager services you want to install. There are three services you can install.

   - **Control Service** – Manages all DocAve operations and communicates with the web-based DocAve platform, allowing users to interact with the software. All agents communicate with the Manager via the Control service, so it is imperative that the machine you install the Control service on is accessible by all agent machines. This service can be run on a Windows Network Load Balanced cluster to ensure load balancing which leverages the Windows Network Load Balancer to automatically select the proper DocAve Control service for optimal performance. For more information, refer to the DocAve Control Service Load BalancingDocAve Control Service section of this guide.
   - **Media Service** – Performs assistant jobs such as managing the retention rules and managing the backup job data. This service can be installed on multiple machines. Using multiple media services allows for load-balanced access to the data storage locations.
   - **Report Service** – Manages all SharePoint data collections and managements, monitor SharePoint activities and return the data to the Control service for processing. This must be configured with the associated SQL databases and SQL Report services. This service is critical for using the DocAve Report Center module.

     ***Note**: DocAve Report service can be installed on multiple servers and can be load balanced. However, all Report services must share the same Report Database and Auditor Database.

   Click **Next**.

7. Set up the **Control Service Configuration:**

   - **IIS Website Settings** – Configure the IIS website settings for the Control service. The IIS website is used to access DocAve Manager.
     - **IIS website** – Enter the website name and create a new IIS website for the Control service. The default **Website Port** used to access DocAve Control service is 14000, you do not need to change it unless a known port conflict exists.
     - **Website Port** – Control service communication port. The default port is 14000.
   - **Application Pool Settings** – Configure the IIS application pool settings for the corresponding website. The application pool is used to handle the requests sent to the corresponding website.
     - **Application pool** – Enter the application pool name for the corresponding website.
     - **Application Pool Account** – Enter an application pool account to be the administrator of the specified application pool, and the corresponding password.

***Note**: The application pool account for connecting an existing IIS website or creating a new IIS website must have the following **Local System Permissions:**

Member of the following local group:

- IIS_WPG (for IIS 6) or IIS_IUSRS (for IIS 7 and IIS 8)
- Full Control to HKEY_LOCAL_MACHINE\SOFTWARE\AvePoint\DocAve6
- Full Control to DocAve Manager folder
- Member of the Performance Monitor Users group
- Full Control to DocAve Certificate private keys
- Full Control (or Read, Write, Modify and Delete) to *C:\WINDOWS\Temp* (only for Windows 2003 environment)

You can add the application pool account to the local **Administrators** group to meet the required permissions.

Click **Next** to continue to configure the database settings for the Control service.

8. Configure a database for storing the relevant data of Control service.
   - **Database Type** – Only MS SQL Server is supported to serve as the database server for Control service.
   - **Database Server** – Enter the MS SQL server name.
   - **Control Database Name** – Enter a database name for the Control service, if the database does not exist, it will be created in the provided MS SQL server.
   - **Database Credentials** – Select the credential for this Control database.
     - **Windows Authentication** (the default option) – Use this method when you want the user identity to be confirmed by Windows. The account must have the following permissions.

       Local Permissions – The user must have the following permission to the machine where the DocAve Manager will be installed: Log on as a batch job (found in **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Security Settings** > **Local Policies** > **User Rights Assignment**).

       SQL Permissions – The user must have the necessary permission to access the SQL Server machine where you want to create the Control database. Also, the user must have the following permission: **db_owner** database role in the existing DocAve 6 Control database or **dbcreator** server role in the SQL Server that will contain the newly created DocAve 6 Control database.

     - **SQL Authentication** – SQL server will confirm the user identity itself according to the specified account and password. The specified account must have the following permission: **db_owner** database role in the existing DocAve 6 Control

database or **dbcreator** server role in the SQL Server that will contain the newly created DocAve 6 Control database.

- **Passphrase Settings** – Enter the passphrase you want to use for protecting DocAve Manager data.
- **Advanced Database Settings** – You can choose to associate the DocAve Control database with a specific failover SQL server that is used in conjunction with SQL Server database mirroring.

Click **Next**.

9. Set up the Media Service Configuration.
    - **Media Service Port** – Used for communicating with the other DocAve services. The default port is 14001.
    - **Media Service Data Port** – Transmit the data between DocAve and the storage device. The default port is 14002.
    - **Use a random port number if the specified one is being used** – Enable this option to have the DocAve Manager installation program generate a random port if the Media Service Port or Media Service Data Port you specified is being used by other applications. If this option is not enabled, the port will not be checked until installation.

    Click **Next**.
10. Set up the **Report Service Configuration**.
    - **Report Service Port** – The port number for Report service. The default port is 14003.
    - **Use a random port number if the specified one is being used** – If enable this option, DocAve Manager installation program will generate a random port if the specified Report Service Port is being used by other applications. If this option is not enabled, the port will not be checked until installation.

    Click **Next** to continue to configure the database settings for Report service.
11. For the report service database, you can select to use the previous database settings or configure it yourself.
    - **Use the previous database settings** – (This option can only be selected once the Control database is configured in the previous step. If you select this option, the previous database settings for Control database will be used for the report database.

      To set a database for report service only, the following information must be configured.
    - **Database Type** – Only MS SQL Server is supported to serve as the database server for Report service.
    - **Database Server** – Enter the MS SQL server name.
    - **Report Database Name** – Enter a database name for the Report service, if the database does not exist, it will be created in the provided MS SQL server.
    - **Database Credentials** – Select the credential for this Report database.

- **Windows Authentication** (the default option) – Use this method when you want the user identity to be confirmed by Windows. The account must have the following permissions.

  Local Permissions – The user must have the following permission to the machine where the DocAve Manager will be installed: Log on as a batch job (found in **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Security Settings** > **Local Policies** > **User Rights Assignment**).

  SQL Permissions – The user must have the necessary permission to access the SQL Server machine where you want to create the Report database. Also, the user must have the following permission: **db_owner** database role in the existing DocAve 6 Report database or **dbcreator** server role in the SQL Server that will contain the newly created DocAve 6 Report database.

- **SQL Authentication** – SQL server will confirm the user identity itself according to the specified account and password. The specified account must have the following permission: **db_owner** database role in the existing DocAve 6 Report database or **dbcreator** server role in the SQL Server that will contain the newly created DocAve 6 Report database.

- **Advanced Database Settings** – You can choose to associate the DocAve Report database with a specific failover SQL server that is used in conjunction with SQL Server database mirroring.

Click **Next** to continue to configure the Auditor database settings for the Report service.

12. For the Auditor database, you can select to use the previous database settings or configure it yourself.

    - **Use the previous database settings** – If you select this option, the previous database server for Control service will be used for the auditor database.

    To set an auditor database for report service only, the following information must be configured.

    - **Database Type** – Only MS SQL Server is supported to serve as the database server for Report service.
    - **Database Server** – Enter the MS SQL server name.

      ***Note**: It is recommended to create the DocAve Auditor database on a different SQL server than the SQL server that stores the SharePoint databases. Since DocAve Auditor Controller retrieves data from the SharePoint Auditor database, if you have DocAve Auditor Controller retrieving data on a frequent schedule, as the amount of data in the SharePoint Auditor database grows, a large amount of disk space will be taken up on the SQL Server machine. This can cause performance issues for both the SQL Server and SharePoint.

- **Auditor Database Name** – Enter a database name for the Auditor database, if the database does not exist, it will be created in the provided MS SQL server.
- **Database Credentials** – Select the credential for this Auditor database.
    - **Windows Authentication** (the default option) – Use this method when you want the user identity to be confirmed by Windows. The account must have the following permissions.

      Local Permissions – The user must have the following permission to the machine where the DocAve Manager will be installed: Log on as a batch job (found in **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Security Settings** > **Local Policies** > **User Rights Assignment**).

      SQL Permissions – The user must have the necessary permissions to access the SQL Server machine where you want to create the Auditor database. Also, the user must have the following permission: **db_owner** database role in the existing DocAve 6 Auditor database or **dbcreator** server role in the SQL Server that will contain the newly created DocAve 6 Auditor database.
    - **SQL Authentication** – SQL server will confirm the user identity itself according to the specified account and password. The specified account must have the following permission: **db_owner** database role in the existing DocAve 6 Auditor database or **dbcreator** server role in the SQL Server that will contain the newly created DocAve 6 Auditor database.
- **Advanced Database Settings** – You can choose to associate the DocAve Auditor database with a specific failover SQL server that is used in conjunction with SQL Server database mirroring.

13. Once all of the required information has been configured, in the Installation Summary page, all of the information configured in the previous steps is listed. Click **Save**, and specify the path you want to save the Answer file to. You can also modify the Answer file's name in the pop-up window.

Import the UnattendedInstallation.dll File

Before performing the DocAve Manager unattended installation, the **UnattendedInstallation.dll** file must be imported into Windows PowerShell using either of the two methods below.

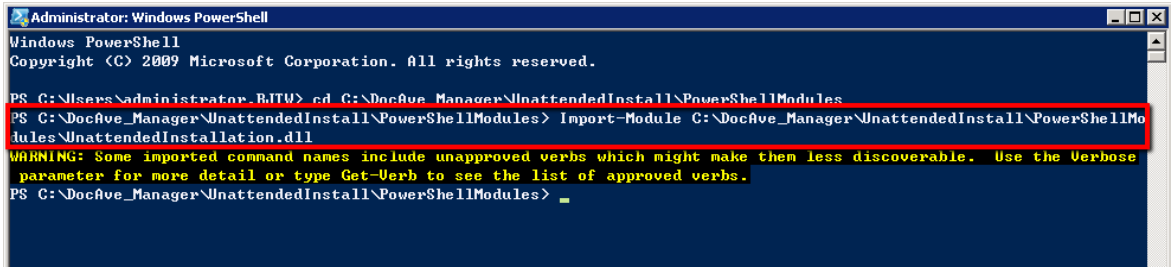
***Note**: If the **UnattendedInstallation.dll** file is not imported successfully, use the **Set-ExecutionPolicy** command to set the execution policy to **Unrestricted**, **RemoteSigned,** or **AllSigned** in Windows PowerShell and perform the import again using one of the following methods.

To manually import the UnattendedInstallation.dll file, complete the following steps:

1. Click **Start** on the server with the unzipped Manager installation package residing in, and find Windows PowerShell. Right click on it, and select **Run as administrator** to run it.

2. Enter the following command, and press **Enter** to import the **UnattendedInstallation.dll** file:

   Import-Module …\UnattendedInstall\PowerShellModules\UnattendedInstallation.dll



   ***Note**: The warning message displayed in the screenshot above is caused by some terminologies in the **UnattendedInstallation.dll** file violating Windows PowerShell's naming convention. It has no effect on file importing. The **UnattendedInstallation.dll** file is imported successfully.

To automatically import the **UnattendedInstallation.dll** file, complete the following steps:

1. Navigate to the *…\UnattendedInstall\PowerShellModules* folder inside the unzipped Manager installation package.
2. Right click on the **UnattendedInstallationLauncher.bat** file, and select **Run as administrator** to run it.

Now that you have imported the UnattendedInstallation.dll file, you can use the commands in the following sections to check your environment, perform the manager installation and configure settings.

Commands and Command Parameters for DocAve Manager Unattended Installation

To perform the DocAve Manager unattended installation, refer to the following sections for the commands.

Environment Checking Command

Before executing DocAve Manager installation command, you can use the **Check-ManagerEnvironment** command to check whether the destination server you want to install DocAve Manager meet the DocAve Manager System Requirements.

For example:

Check-ManagerEnvironment -TargetName *Hostmachine* **-Username** *AvePoint\DocAve* **-Password** *"Ave"* **-CheckEnvironmentFilePath** *"C:\DocAve_Manager\DocAve.dat"* **-AnswerFilePath** *"C:\AnswerFile.xml"*

This table contains detailed information for each of the parameters:

Parameter	Type	Description
-TargetName	Required	The name or IP address of the destination machine where you want to install the DocAve Manager.

Parameter	Type	Description
		***Note**: If the hostname is used, ensure that the specified computer name can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.
-Username	Required	The username of the user used to access the destination machine where you want to install the DocAve Manager. The format of the username is: domain\username. The permissions of the user specified here are as follows: • If the specified user is the local administrator of the destination machine, it can be used directly. Enter .*administrator* for the *Username* parameter. • If the specified user is from the domain which the destination machine belongs to, the domain user must be added to the **Administrators** group on the destination machine. The user specified here must have the Full Control permission to the path specified in *RemoteTempPath* parameter.
-Password	Required	The password of the user specified above. Quote the password if it contains any special character or space.
-CheckEnvironmentFilePath	Required	The local path of the DocAve.dat file that is residing in the unzipped DocAve Manager installation package. The path must be detailed to the name of the data file. For example, *C:\DocAve_Manager\ DocAve.dat*.
-AnswerFilePath	Required	The local path where you saved the Answer file. The path must be detailed to the name of the Answer file. For example, *C:\AnswerFileManager.xml*.
-RemoteTempPath	Required	A local path on the destination machine that the DocAve Manager is installed to. The format of the path is: C:\temp. The path will be used to store the temporary files generated during the DocAve Manager unattended installation. The temporary files will be deleted as soon as the unattended installation finishes.

Parameter	Type	Description
-Log	Optional	This is an optional parameter. If used, the environment checking logs will be saved to the .txt file in the specified path. The generated log file is a text file. The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Log.txt.* If the specified log file does not exist, it will be generated automatically.
-ProductType	Required	This parameter is used to identify the product you are installing from other AvePoint's products. Enter **DocAve** as the value of this parameter when you install DocAve products.
-UseIPv6forCommunication	Optional	This is an optional parameter used to specify the communication method between the machine where the command is run and the destination machine that the DocAve Manager is installed. If an IPv6 address is entered in **TargetName** parameter, this parameter must be entered. ***Note**: When using this parameter, both the destination machine and the machine where you run this command must support IPv6.
-ReceiveInfoPort	Optional	This is an optional parameter to specify a port for the source machine to receive the data from the destination machine. This port and the destination machine's IP are added to an inbound rule of the source machine's firewall so it allows all the connections from the destination machine. DocAve recommends you configure this parameter to ensure smooth communication between the source machine and the destination machine.
-Timeout	Optional	This is an optional parameter to specify a timeout value for waiting for the return message from the destination machine. A timeout error will occur if there is no message returned from the destination machine in the specified period.
-ReceiveInfoIP	Optional	If multiple IP addresses have been configured on the source machine, use this parameter to specify an IP address for the source machine to communicate with the destination machine.

Installation Command

The DocAve Manager Unattended Installation command for installing DocAve Manager remotely is **Install-DAManager**. For example:

Install-DAManager -TargetName *hostmachine* **-Username** *AvePoint\DocAve* **-Password** *"Ave"* **-PackageFilesFolder** *"C:\DocAve_Manager"* **-AnswerFilePath** *"C:\AnswerFile.xml"* **-RemoteTempPath** *"C:\TempFolder"* **-ProductType** *"DocAve"*

This table contains detailed information for each of the parameters:

Parameter	Type	Description
-TargetName	Required	The name or IP address of the destination machine where you want to install the DocAve Manager. ***Note**: If the hostname is used, ensure that the specified computer name can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.
-Username	Required	The username of the user used to access the destination machine where you want to install the DocAve Manager. The format of the username is: domain\username. The permissions of the user specified here are as follows: • If the specified user is the local administrator of the destination machine, it can be used directly. Enter *.\administrator* for the *Username* parameter. • If the specified user is from the domain which the destination machine belongs to, the domain user must be added to the **Administrators** group on the destination machine. The user specified here must have the Full Control permission to the path specified in *RemoteTempPath* parameter.
-Password	Required	The password of the user specified above.

Parameter	Type	Description
		Quote the password if it contains any special character or space.
-PackageFilesFolder	Required	The local path on the machine where you run the command. The specified path stores the unzipped DocAve Manager installation package (Manager ZIP file). The format of the path is: *C:\package*. Quote the path if it contains any special character or space.
-AnswerFilePath	Required	The local path where you saved the Answer file. The path must be detailed to the name of the Answer file. For example, *C:\AnswerFile.xml*.
-RemoteTempPath	Required	A local path on the destination machine that the DocAve Manager is installed to. The format of the path is: *C:\temp*. The path will be used to store the temporary files generated during the DocAve Manager unattended installation. The temporary files will be deleted as soon as the unattended installation finishes.
-Log	Optional	This is an optional parameter. If used, the logs of the unattended installation will be saved to the .txt file in the specified path. The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Log.txt.* If the specified log file does not exist, it will be generated automatically.
-UseIPv6forCommunication	Optional	This is an optional parameter used to specify the communication method between the machine where the command is run and the destination machine that the DocAve Manager is installed. If an IPv6 address is entered in **TargetName** parameter, this parameter must be entered. ***Note**: When using this parameter, both the destination machine and the machine where you run this command must support IPv6.

Parameter	Type	Description
-ProductType	Required	This parameter is used to identify the product you are installing from other AvePoint's products. Enter **DocAve** as the value of this parameter when you install DocAve products.
-ReceiveInfoPort	Optional	This is an optional parameter to specify a port for the source machine to receive the data from the destination machine. This port and the destination machine's IP are added to an inbound rule of the source machine's firewall so it allows all the connections from the destination machine. DocAve recommends you configure this parameter to ensure smooth communication between the source machine and the destination machine.
-Timeout	Optional	This is an optional parameter to specify a timeout value for waiting for the return message from the destination machine. A timeout error will occur if there is no message returned from the destination machine in the specified period.
-ReceiveInfoIP	Optional	If multiple IP addresses have been configured on the source machine, use this parameter to specify an IP address for the source machine to communicate with the destination machine.

Getting Configuration Information Command

The **Get-DAManagerConfigInfo** command allows you to remotely get the configuration information of DocAve Manager. You can not only get the configuration information of the Managers installed remotely through the use of Unattended Installation, but also can get the configuration information of the Managers installed locally through the use of installation wizard. In a word, you are able to remotely get the configuration information of any Managers.

An example of the **Get-DAManagerConfigInfo** command is:

Get-DAManagerConfigInfo -TargetName *hostmachine* **-Username** *AvePoint\DocAve* **-Password** *"Ave"*

This table contains detailed information for each of the parameters:

Parameter	Type	Description
-TargetName	Required	The name or IP address of the destination machine where has DocAve Manager installed. ***Note**: If the hostname is used, ensure that the specified computer name can be resolved through the local Hosts

Parameter	Type	Description
		file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.
-Username	Required	The username of the user used to access the destination machine where has DocAve Manager installed. The format of the username is: domain\username. The permissions of the user specified here are as follows: • If the specified user is the local administrator of the destination machine, it can be used directly. Enter .*administrator* for the *Username* parameter. • If the specified user is from the domain which the destination machine belongs to, the domain user must be added to the **Administrators** group on the destination machine. The user specified here must have the Full Control permission to the path specified in *RemoteTempPath* parameter.
-Password	Required	The password of the user specified above. Quote the password if it contains any special character or space.
-Log	Optional	This is an optional parameter. If used, the configuration information logs will be saved to the .txt file in the specified path. The generated log file is a text file. The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Log.txt.* If the specified log file does not exist, it will be generated automatically.
-AnswerFilePath	Optional	This is an optional parameter. If used, the configuration information you get by the **Get-DAManagerConfigInfo** command will be exported to the .xml file in the specified path. Only the .xml file is supported by this parameter. The content format of the generated .xml file is the same as the Manager Answer File. The path specified in this parameter must be detailed to the name of the log file. For example, *C:\ManagerConfigInfor.xml.*

Parameter	Type	Description
		There must be no .xml file with the same name existing in the specified path.
-ProductType	Required	This parameter is used to identify the product you are getting the configuration information from other AvePoint's products. Enter *DocAve* as the value of this parameter when you install DocAve products.
-UseIPv6forCommunication	Optional	This is an optional parameter used to specify the communication method between the machine where the command is run and the destination machine that the DocAve Manager is installed. If an IPv6 address is entered in **TargetName** parameter, this parameter must be entered. ***Note**: When using this parameter, both the destination machine and the machine where you run this command must support IPv6.
-ReceiveInfoPort	Optional	This is an optional parameter to specify a port for the source machine to receive the data from the destination machine. This port and the destination machine's IP are added to an inbound rule of the source machine's firewall so it allows all the connections from the destination machine. DocAve recommends you configure this parameter to ensure smooth communication between the source machine and the destination machine.
-Timeout	Optional	This is an optional parameter to specify a timeout value for waiting for the return message from the destination machine. A timeout error will occur if there is no message returned from the destination machine in the specified period.
-ReceiveInfoIP	Optional	If multiple IP addresses have been configured on the source machine, use this parameter to specify an IP address for the source machine to communicate with the destination machine.

Configuring Configuration Information Command

The **Config-DAManagerConfigInfo** command allows you to remotely modify the configuration information of DocAve Manager. You can not only modify the configuration information of the Managers installed remotely through the use of Unattended Installation, but also can modify the

configuration information of the Managers installed locally through the use of installation wizard. In a word, you are able to remotely modify the configuration information of any Managers.

For example:

Config-DAManagerConfigInfo *-TargetName hostmachine* **-Username** *AvePoint\DocAve* **-Password** *"Ave"* **-UseControlFailoverDatabse** *true* **-UseWindowsAuthenticationForControlDatabase** *true* **UseReportFailoverDatabase** true

This table contains detailed information for each of the parameters:

Parameter	Type	Description
-TargetName	Required	The name or IP address of the destination machine where has the DocAve Manager installed. ***Note**: If the hostname is used, ensure that the specified computer name can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.
-Username	Required	The username of the user used to access the destination machine where the DocAve Manager is installed. The format of the username is: domain\username. The permissions of the user specified here are as follows: • If the specified user is the local administrator of the destination machine, it can be used directly. Enter *.\administrator* for the *Username* parameter. • If the specified user is from the domain which the destination machine belongs to, the domain user must be added to the **Administrators** group on the destination machine. The user specified here must have the Full Control permission to the path specified in *RemoteTempPath* parameter.
-Password	Required	The password of the user specified above. Quote the password if it contains any special character or space.

Parameter	Type	Description
-ControlServiceHost	Optional	If the host or IP of the destination server that has Control service installed is changed, use this parameter to change the host or IP of the Control service to the new one.
-WebsiteName	Optional	The name of the new website you want to use for the DocAve Manager Control service installed on the destination machine. You can use an existing IIS website or create a new IIS website.
-WebSitePort	Optional	The new website port you want to use for the DocAve Manager installed on the destination machine.
-ApplicationPoolName	Optional	The name of the new application pool you want to use for the IIS website for the DocAve Control service. You can either use an existing application pool or create a new one. If you want to create a new application pool with this parameter, you must specify the username and password of the account to authenticate the application pool with the two parameters below.
–ApplicationPoolUsername	Optional	The username of the new account you want to use to authenticate the application pool specified above. ***Note**: If you create a new application pool with-**ApplicationPoolName**, **–ApplicationPoolUsername** must be configured.
–ApplicationPoolPassword	Optional	The password of the account to authenticate the specified application pool. ***Note**: If you create a new application pool with-**ApplicationPoolName**, **–ApplicationPoolUsername** must be configured.
-ControlDatabaseServer	Optional	The new server you want to use for the Control database. ***Note**: The specified server must have an existing database of the same type with the Control database. And you must configure the passphrase for the new Control database with **–ControlPassphrase**.
-ControlDatabaseName	Optional	The new database you want to use as the Control database. ***Note**: The specified database must be an existing database of the same type with the Control database. And you must configure the passphrase for the new Control database with **–ControlPassphrase**.
-ControlPassphrase	Optional	The passphrase for the Control database specified above. ***Note**: If **–ControlDatabaseServer** or **–ControlDatabaseName** is used, **-ControlPassphrase** must be configured.

Parameter	Type	Description
-UseControlFailoverDatabase	Optional	Enable the failover database server function for the Control database. If the Control database on the destination machine is not associating a failover database server, set the value of this parameter to *True* allows you to specify a failover database server in the following parameter.
-ControlFailoverDatabase	Optional	The failover SQL server you want to associate to the Control database. ***Note**: If the parameter **–UseControlFailoverDatabase** is used, -**ControlFailoverDatabase** must be configured.
-UseWindowsAuthenticationForControlDatabase	Optional	Using this parameter to change the authentication of the Control service database between Windows Authentication and SQL Authentication. If the current authentication being used in the destination Control service database is Windows Authentication, you can set the value of this parameter to *False* to change the authentication to SQL Authentication, and vise verse.
-ControlDatabaseUsername	Optional	The new account you want to use to authenticate the Control service database on the destination machine. ***Note**: If the parameter **–UseWindowsAuthenticationForControlDatabase** is used, **-ControlDatabaseUsername** must be configured.
-ControlDatabasePassword	Optional	The password of the user specified above. ***Note**: If the parameter **–UseWindowsAuthenticationForControlDatabase** is used, **-ControlDatabasePassword** must be configured. Quote the password if it contains any special character or space.
-MediaServiceHost	Optional	If the host or IP of the destination server that has Media service installed is changed, use this parameter to change the host or IP of the Media service to the new one.
-MediaServicePort	Optional	The new Media service port you want to use for the Media service.
-MediaServiceDataPort	Optional	The new Media service data port you want to use for the Media service.
-MediaControlServiceHost	Optional	If the host of the Control service that the Media service is registered in is changed, use this parameter to change the host of the Control service to the new one.

Parameter	Type	Description
-MediaControlServicePort	Optional	If the port of the Control service that the Media service is registered in is changed, use this parameter to change the port of the Control service to the new one.
-ReportServiceHost	Optional	If the host or IP of the destination server that has Report service installed is changed, use this parameter to change the host or IP of the Report service to the new one.
-ReportServicePort	Optional	The new port you want to use for the Report service.
-ReportControlServiceHost	Optional	If the host of the Control service that the Report service is registered in is changed, use this parameter to change the host of the Control service to the new one.
-ReportDatabaseServer	Optional	The new server you want to use for the Report database. ***Note**: The specified server must have an existing database of the same type with the Report database.
-ReportDatabaseName	Optional	The new database you want to use as the Report database. ***Note**: The specified database must be an existing database of the same type with the Report database.
-ReportControlServicePort	Optional	If the port of the Control service that the Report service is registered in is changed, use this parameter to change the port of the Control service to the new one.
-UseReportFailoverDatabase	Optional	Enable the failover database server function for the Report database. If the Report database on the destination machine is not associating a failover database server, set the value of this parameter to *True* allows you to specify a failover database server in the following parameter.
-ReportFailoverDatabase	Optional	The failover SQL server you want to associate to the Report database. ***Note**: if the parameter **– UseReportFailoverDatabase** is used, **– ReportFailoverDatabase** must be configured.
-UseWindowsAuthenticationForReportDatabase	Optional	Using this parameter to change the authentication of the Report database between Windows Authentication and SQL Authentication. If the current authentication being used in the destination Report database is Windows Authentication, you can set the value of this parameter to *False* to change the authentication to SQL Authentication, and vise verse.

Parameter	Type	Description
-ReportDatabaseUsername	Optional	The new account you want to use to authenticate the Report database on the destination machine. *__Note__: If the parameter __–UseWindowsAuthenticationForReportDatabase__ is used, the __–ReportDatabaseUsername__ must be configured.
-ReportDatabasePassword	Optional	The password of the user specified above. *__Note__: If the parameter __–UseWindowsAuthenticationForReportDatabase__ is used, the __–ReportDatabasePassword__ must be configured. Quote the password if it contains any special character or space.
-AuditorDatabaseServer	Optional	The new server you want to use for the Auditor database. ***Note**: The specified server must have an existing database of the same type with the Auditor database.
-AuditorDatabaseName	Optional	The new database you want to use as the Auditor database. ***Note**: The specified database must be an existing database of the same type with the Auditor database.
-UseAuditorFailoverDatabase	Optional	Enable the failover database server function for the Auditor database. If the Auditor database on the destination machine is not associating a failover database server, set the value of this parameter to *True* allows you to specify a failover database server in the following parameter.
-AuditorFailoverDatabase	Optional	The failover SQL server you want to associate to the Auditor database. *__Note__: If the parameter __–UseAuditorFailoverDatabase__ is used, the __–AuditorFailoverDatabase__ must be configured.
-UseWindowsAuthenticationForAuditorDatabase	Optional	Using this parameter to change the authentication of the Auditor database between Windows Authentication and SQL Authentication. If the current authentication being used in the destination Auditor database is Windows Authentication, you can set the value of this parameter to *False* to change the authentication to SQL Authentication, and vise verse.
-AuditorDatabaseUsername	Optional	The new account you want to use to authenticate the Auditor database on the destination machine. *__Note__: If the parameter __–UseWindowsAuthenticationForAuditorDatabase__ is

Parameter	Type	Description
		used, the **–AuditorDatabaseUsername** must be configured.
-AuditorDatabasePassword	Optional	The password of the user specified above. ***Note**: If the parameter **–UseWindowsAuthenticationForAuditorDatabase** is used, the **–AuditorDatabasePassword** must be configured. Quote the password if it contains any special character or space.
-Log	Optional	This is an optional parameter. If used, the configuration information logs will be saved to the .txt file in the specified path. The generated log file is a text file. The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Log.txt.* If the specified log file does not exist, it will be generated automatically.
-ProductType	Required	This parameter is used to identify the product you are configuring from other AvePoint's products. Enter *DocAve* as the value of this parameter when you install DocAve products.
-UseIPv6forCommunication	Optional	This is an optional parameter used to specify the communication method between the machine where the command is run and the destination machine that the DocAve Manager is installed. If an IPv6 address is entered in **TargetName** parameter, this parameter must be entered. ***Note**: When using this parameter, both the destination machine and the machine where you run this command must support IPv6.
-ReceiveInfoPort	Optional	This is an optional parameter to specify a port for the source machine to receive the data from the destination machine. This port and the destination machine's IP are added to an inbound rule of the source machine's firewall so it allows all the connections from the destination machine. DocAve recommends you configure this parameter to ensure

Parameter	Type	Description
		smooth communication between the source machine and the destination machine.
-Timeout	Optional	This is an optional parameter to specify a timeout value for waiting for the return message from the destination machine. A timeout error will occur if there is no message returned from the destination machine in the specified period.
-ReceiveInfoIP	Optional	If multiple IP addresses have been configured on the source machine, use this parameter to specify an IP address for the source machine to communicate with the destination machine.

Verifying Configuration Information Command

The **Verify-DAManagerConfigInfo** command allows you to remotely verify that the configuration information you want to use for DocAve Manager is valid. You can verify the configuration information for the Managers installed remotely through the use of Unattended Installation and the configuration information for the Managers installed locally with the installation wizard.

An example of the **Verify-DAManagerConfigInfo** command is:

Verify -DAManagerConfigInfo *-TargetName hostmachine* **-Username** *AvePoint\DocAve* **-Password** *"Ave"* **-UseControlFailoverDatabse** *true* **-UseWindowsAuthenticationForControlDatabase** *true* **UseReportFailoverDatabase** true

This table contains detailed information for each of the parameters:

Parameter	Type	Description
-TargetName	Required	The name or IP address of the destination machine where has the DocAve Manager installed. ***Note**: If the hostname is used, ensure that the specified computer name can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.
-Username	Required	The username of the user used to access the destination machine where you want to install the DocAve Manager. The format of the username is: domain\username. The permissions of the user specified here are as follows: • If the specified user is the local administrator of the destination machine, it can be used directly. Enter *.\administrator* for the *Username* parameter.

Parameter	Type	Description
		• If the specified user is from the domain which the destination machine belongs to, the domain user must be added to the **Administrators** group on the destination machine. The user specified here must have the Full Control permission to the path specified in *RemoteTempPath* parameter.
-Password	Required	The password of the user specified above. Quote the password if it contains any special character or space.
-ControlServiceHost	Optional	The Control service host or IP you want to verify for the destination machine.
-WebsiteName	Optional	The name of the new website you want to verify for the DocAve Manager Control service installed on the destination machine. You can verify an existing IIS website or a new IIS website needed to be created.
-WebSitePort	Optional	The website port you want to verify for the DocAve Manager installed on the destination machine.
-ApplicationPoolName	Optional	The name of the new application pool you want to verify for the IIS website for the DocAve Control service. You can either verify an existing application pool or a new one to be created. If you want to verify a new application pool to be created, you must specify the username and password of the account to authenticate the application pool with the two parameters below.
-ApplicationPoolUsername	Optional	The username of the new account you want to verify to authenticate the application pool specified above. ***Note**: If you want to verify a new application pool to be created with-**ApplicationPoolName**, **–ApplicationPoolUsername** must be configured.
–ApplicationPoolPassword	Optional	The password of the account to authenticate the specified application pool. ***Note**: If you want to verify a new application pool to be created with-**ApplicationPoolName**, **–ApplicationPoolUsername** must be configured.
-ControlDatabaseServer	Optional	The new server you want to verify for the Control database. ***Note**: The specified server must have an existing database of the same type with the Control database. And you must configure the passphrase for the new Control database with **–ControlPassphrase**.
-ControlDatabaseName	Optional	The new database you want to verify as the Control database.

Parameter	Type	Description
		***Note**: The specified database must be an existing database of the same type with the Control database. And you must configure the passphrase for the new Control database with **–ControlPassphrase**.
-ControlPassphrase	Optional	The passphrase for the Control database specified above. ***Note**: If **–ControlDatabaseServer** or **–ControlDatabaseName** is used, **-ControlPassphrase** must be configured.
-UseControlFailoverDatabse	Optional	Set *True* as the value of this parameter and verify whether you can specify a failover SQL Server for the Control database.
-ControlFailoverDatabse	Optional	Set the host or IP address of the failover SQL Server as the value of this parameter and verify whether the specified SQL Server is available.
-UseWindowsAuthenticationForControlDatabase	Optional	Set *True* or *False* as the value of this parameter and verify whether you can use Windows Authentication for the Control database.
-ControlDatabaseUsername	Optional	Verifying the account you want to use to authenticate the Control database on the destination machine.
-ControlDatabasePassword	Optional	Verifying the password for the specified account above. Quote the password if it contains any special character or space.
-MediaServiceHost	Optional	The Media service host or IP you want to verify for the destination machine.
-MediaServicePort	Optional	The Media service port you want to verify for the DocAve Manager installed on the destination machine.
-MediaServiceDataPort	Optional	The Media service port you want to verify for the DocAve Manager installed on the destination machine.
-MediaControlServiceHost	Optional	Verifying the host or IP of the Control service that the Media service is registered in.
-MediaControlServicePort	Optional	Verifying the port of the Control service that the Media service is registered in.
-ReportServiceHost	Optional	The Report service host or IP you want to verify for the destination machine.
-ReportServicePort	Optional	The Report service port you want to verify for the DocAve Manager installed on the destination machine.
-ReportControlServiceHost	Optional	Verifying the host or IP of the Control service that the Report service is registered in.
-ReportControlServicePort	Optional	Verifying the port of the Control service that the Report service is registered in.
-ReportDatabaseServer	Optional	The new server you want to verify for the Report database. ***Note**: The specified server must have an existing database of the same type with the Report database.

Parameter	Type	Description
-ReportDatabaseName	Optional	The new database you want to verify as the Report database. ***Note**: The specified database must be an existing database of the same type with the Report database.
-UseReportFailoverDatabase	Optional	Set *True* as the value of this parameter and verify whether you can specify a failover SQL Server for the Report database.
-ReportFailoverDatabase	Optional	Set the host or IP address of the failover SQL Server as the value of this parameter and verify whether the specified SQL Server is available.
-UseWindowsAuthenticationForReportDatabase	Optional	Set *True* or *False* as the value of this parameter and verify whether you can use Windows Authentication for the Report database.
-ReportDatabaseUsername	Optional	Verifying the account you want to use to authenticate the Report database on the destination machine.
-ReportDatabasePassword	Optional	Verifying the password for the specified account above. Quote the password if it contains any special character or space.
-AuditorDatabaseServer	Optional	The new server you want to verify for the Auditor database. ***Note**: The specified server must have an existing database of the same type with the Auditor database.
-AuditorDatabaseName	Optional	The new database you want to verify as the Auditor database. ***Note**: The specified database must be an existing database of the same type with the Auditor database.
-UseAuditorFailoverDatabase	Optional	Set *True* as the value of this parameter and verify whether you can specify a failover SQL Server for the Auditor database.
-AuditorFailoverDatabase	Optional	Set the host or IP address of the failover SQL Server as the value of this parameter and verify whether the specified SQL Server is available.
-UseWindowsAuthenticationForAuditorDatabase	Optional	Set *True* or *False* as the value of this parameter and verify whether you can use Windows Authentication for the Auditor database.
-AuditorDatabaseUsername	Optional	Verifying the account you want to use to authenticate the Auditor Service database on the destination machine.
-AuditorDatabasePassword	Optional	Verifying the password for the specified account above. Quote the password if it contains any special character or space.
-Log	Optional	This is an optional parameter. If used, the verifying configuration log information will be saved to the .txt file in the specified path. The generated log file is a text file.

Parameter	Type	Description
		The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Log.txt.* If the specified log file does not exist, it will be generated automatically.
-ProductType	Required	This parameter is used to identify the product whose configuration information you are verifying from other AvePoint's products. Enter *DocAve* as the value of this parameter when you install DocAve products.
-UseIPv6forCommunication	Optional	This is an optional parameter used to specify the communication method between the machine where the command is run and the destination machine that the DocAve Manager is installed. If an IPv6 address is entered in **TargetName** parameter, this parameter must be entered. ***Note**: When using this parameter, both the destination machine and the machine where you run this command must support IPv6.
-ReceiveInfoPort	Optional	This is an optional parameter to specify a port for the source machine to receive the data from the destination machine. This port and the destination machine's IP are added to an inbound rule of the source machine's firewall so it allows all the connections from the destination machine. DocAve recommends you configure this parameter to ensure smooth communication between the source machine and the destination machine.
-Timeout	Optional	This is an optional parameter to specify a timeout value for waiting for the return message from the destination machine. A timeout error will occur if there is no message returned from the destination machine in the specified period.
-ReceiveInfoIP	Optional	If multiple IP addresses have been configured on the source machine, use this parameter to specify an IP address for the source machine to communicate with the destination machine.

Getting Help Information About DocAve Manager Unattended Installation Commands

Once you have imported the UnattendedInstallation.dll file, you can use the **Get-Help** command to get help information about any of the above DocAve Manager Unattended Installation commands. This command enables you to get comprehensive information for the specified command, including the syntax, description, detailed information for each parameter**,** and examples.

For example, if you want to get the help information of the **Install-DAManager** command, enter the following command:

Get-Help *Install-DAManager* **–Full**

Unattended Installation of DocAve Agent

The DocAve Agent can be installed remotely using the unattended installation after the Manager's services have started.

Make sure the system requirements are met before starting the DocAve Agent unattended installation. For more information, refer to System Requirements for Agent Service Installation.

For more information on where to install the DocAve Agents, refer to Appendix A: Where to Install DocAve Agents.

Generating the Installation Answer File for DocAve Agent

The Answer file is an XML file which provides configuration information required for the unattended installation. Before performing the unattended installation, the Answer file must be generated using the DocAve 6 Setup Manager.

Navigate to the **…\UnattendedInstall\SetupManager** folder inside the unzipped Manager installation package, and double click *SetupManager.exe* to run it. You will be guided through the following steps.

1. After being presented with the welcome screen, click **Next**.
2. Select **Create a new answer file for DocAve 6 Agent** to create a new Answer file for DocAve Agent

    - **Modify an existing answer file** – Select this option to reuse an existing Answer file. If this is selected, the path field will be enabled. Enter the full path of the answer file or click **Browse** to browse for an answer file. For example, C:\AnswerFile.xml

    ***Note**: We recommend you create a generic Answer file so that it can be reused later with modification.

3. Click **Next**.

4. Carefully review the DocAve License Agreement.

   After you have read the terms in the license agreement, click on the check-box to select **I accept the terms in the license agreement.** Click **Next**.

5. Enter your name and the organization into the provided field. Click **Next** to continue the configuration. Click **Back** to go back to the previous interface.

6. Set up the installation location using the following conditions.

   - **Default Directory** – The DocAve Agent will be installed to the default installation location on the specified destination server, which is … *\Program Files\AvePoint\DocAve6\Agent.*
   - **Customized Directory** – If select this option, the **Installation Path** field will be enabled, enter a customized path and the DocAve Agent will be installed to the specified path on the destination server.
     - Use the default directory if your customized directory is invalid – If this option is selected, the DocAve Agent will be installed to the default directory when the customized directory is invalid. For example, the path you specified is on a drive which does not exist on the destination server.

   Click **Next**.

7. Set up the **Control Service Configuration**:

   - **DocAve 6 Control Service Host** – The hostname or IP address of the machine where installed Control service.
   - **DocAve 6 Control Service Port** – This is the port used for communication with Control service and should match the information provided during the Manager configuration. The default port number is 14000.

   Click **Next**.

8. Set up the **Agent port**:

   - **DocAve 6 Agent Port** – The port specified here is used by the Manager or other Agents for communication. The default port number is 14004.
     - **Use a random port number if the specified one is being used** – If select this option, DocAve will use a random port number if the port you specified has already been used. This option is selected by default.

   Click **Next**.

9. Set up the Agent configuration:

   - **Manager Passphrase** – Enter the Manager Passphrase specified when configuring the DocAve Manager installation answer file.

- **DocAve Agent Account** – Specify the username and password of the Agent account under which the Agent activities are performed. Refer to Installing DocAve Agent for the detailed permissions required for this account.

10. Click **Next** to access the **Installation Summary** page.
11. After all of the required information has been configured click **Save**, and enter the path you want to save the Answer file to. You can also modify the Answer file's name in the pop-up window.

Import the UnattendedInstallation.dll File

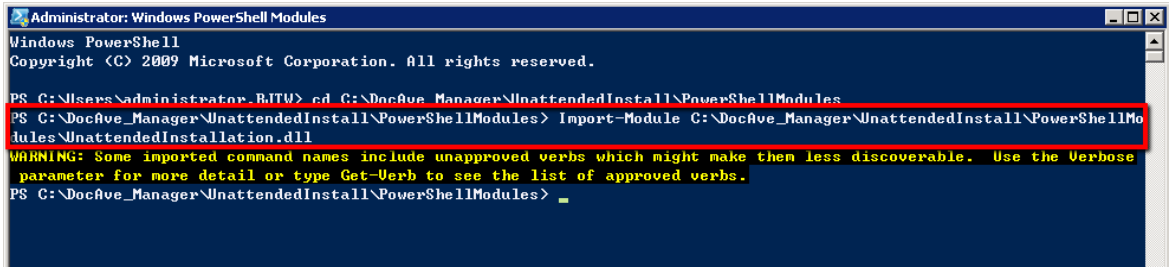
Before performing the DocAve Agent unattended installation, the **UnattendedInstallation.dll** file must be imported into Windows PowerShell using either of the two methods below.

***Note**: If the **UnattendedInstallation.dll** file is not imported successfully, use the **Set-ExecutionPolicy** command to set the execution policy to **Unrestricted**, **RemoteSigned**, or **AllSigned** in Windows PowerShell and perform the import again using either of the two methods below.

To manually import the **UnattendedInstallation.dll** file, complete the following steps:

1. Click **Start**, and find Windows PowerShell. Right click on it, and select **Run as administrator** to run it.
2. Enter the following command, and press **Enter** to import the **UnattendedInstallation.dll** file:

   Import-Module …\UnattendedInstall\PowerShellModules\UnattendedInstallation.dll



   ***Note**: The warning message displayed in the screenshot above is caused by some terminologies in the **UnattendedInstallation.dll** file violating Windows PowerShell's naming convention. It has no effect on file importing. The **UnattendedInstallation.dll** file is imported successfully.

To automatically import the **UnattendedInstallation.dll** file, complete the following steps:

1. Navigate to the …*UnattendedInstall**PowerShellModules* folder inside the unzipped Manager installation package.
2. Right click on the **UnattendedInstallationLauncher.bat** file, and select **Run as administrator** to run it.

   ***Note**: The value of the **Set-ExecutionPolicy** of the Powershell must be set as **AllSigned**.

Now that you have imported the UnattendedInstallation.dll file, you can use the commands in the following sections to check your environment, perform the agent installation and configure settings.

Commands and Command Parameters for DocAve Agent Unattended Installation

To perform the DocAve Agent unattended installation, run the commands in the following sections.

Environment Checking Command

Before executing DocAve Agent installation command, you can use the **Check-AgentEnvironment** command to check whether the destination server you want to install DocAve Agent meet DocAve Agent System Requirements.

An example of the **Check-AgentEnvironment** command is:

Check-AgentEnvironment -TargetName *hostmachine* **-Username** *AvePoint\DocAve* **-Password** *"Ave"* **-CheckEnvironmentFilePath** *"C:\DocAve_Agent\DocAve.dat"* **-AnswerFilePath** *"C:\AnswerFileAgent.xml"*

This table contains detailed information for each of the parameters:

Parameter	Type	Description
-TargetName	Required	The name or IP address of the destination machine where you want to install the DocAve Agent. ***Note**: If the hostname is used, ensure that the specified computer name can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.
-Username	Required	The username of the user used to access the destination machine where you want to install the DocAve Agent. The format of the username is: domain\username. The permissions of the user specified here are as follows: • If the specified user is the local administrator of the destination machine, it can be used directly. Enter *.\administrator* for the *Username* parameter. • If the specified user is from the domain which the destination machine belongs to, the domain user must be added to the

Parameter	Type	Description
		Administrators group on the destination machine. The user specified here must have the Full Control permission to the path specified in *RemoteTempPath* parameter.
-Password	Required	The password of the user specified above. Quote the password if it contains any special character or space.
-CheckEnvironmentFilePath	Required	The local path of the DocAve.dat file that is residing in the unzipped DocAve Agent installation package. The path must be detailed to the name of the data file. For example, C:\DocAve_Agent\ DocAve.dat.
-AnswerFilePath	Required	The local path where you saved the Answer file. The path must be detailed to the name of the Answer file. For example, C:\AnswerFileAgent.xml.
-RemoteTempPath	Required	A local path on the destination machine that the DocAve Agent is installed to. The format of the path is: C:\temp. The path will be used to store the temporary files generated during the DocAve Agent unattended installation. The temporary files will be deleted as soon as the unattended installation finishes.
-Log	Optional	This is an optional parameter. If used, the environment checking logs will be saved to the .txt file in the specified path. The generated log file is a text file. The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Log.txt.* If the specified log file does not exist, it will be generated automatically.
-ProductType	Required	This parameter is used to identify the product you are installing from other AvePoint's products. Enter *DocAve* as the value of this parameter when you install DocAve products.

Parameter	Type	Description
-UseIPv6forCommunication	Optional	This is an optional parameter used to specify the communication method between the machine where the command is run and the destination machine that the DocAve Agent is installed. If an IPv6 address is entered in **TargetName** parameter, this parameter must be entered. ***Note**: When using this parameter, both the destination machine and the machine where you run this command must support IPv6.
-ReceiveInfoPort	Optional	This is an optional parameter to specify a port for the source machine to receive the data from the destination machine. This port and the destination machine's IP are added to an inbound rule of the source machine's firewall so it allows all the connections from the destination machine. DocAve recommends you configure this parameter to ensure smooth communication between the source machine and the destination machine.
-Timeout	Optional	This is an optional parameter to specify a timeout value for waiting for the return message from the destination machine. A timeout error will occur if there is no message returned from the destination machine in the specified period.
-ReceiveInfoIP	Optional	If multiple IP addresses have been configured on the source machine, use this parameter to specify an IP address for the source machine to communicate with the destination machine.

Installation Command

The DocAve Agent Unattended Installation command for installing DocAve Agent remotely is **Install-DAAgent**.

For example:

Install-DAAgent -TargetName *hostmachine* **-Username** *AvePoint\DocAve* **-Password** *"Ave"* **-PackageFilesFolder** *"C:\DocAve_Agent"* **-AnswerFilePath** *"C:\AnswerFile.xml"* **-RemoteTempPath** *"C:\TempFolder"* **-ProductType** *"DocAve"*

The detailed information of the parameters is listed below:

Parameter	Type	Description
-TargetName	Required	The name or IP address of the destination machine where you want to install the DocAve Agent. ***Note**: If the hostname is used, ensure that the specified computer name can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.
-Username	Required	The username of the user used to access the destination machine where you want to install the DocAve Agent. The format of the username is: domain\username. The permissions of the user specified here are as follows: • If the specified user is the local administrator of the destination machine, it can be used directly. Enter .*administrator* for the *Username* parameter. • If the specified user is from the domain which the destination machine belongs to, the domain user must be added to the **Administrators** group on the destination machine. • The user specified here must have the Full Control permission to the path specified in *RemoteTempPath* parameter.
-Password	Required	The password of the user specified above. Quote the password if it contains any special character or space.
-PackageFilesFolder	Required	The local path on the machine where you run the command. The specified path stores the unzipped DocAve Agent installation package (Agent ZIP file). The format of the path is: C:\package. Quote the path if it contains any special character or space.
-AnswerFilePath	Required	The local path where you saved the Answer file.

Parameter	Type	Description
		The path must be detailed to the name of the Answer file. For example, C:\AnswerFile.xml.
-RemoteTempPath	Required	A local path on the destination machine that the DocAve Agent is installed to. The format of the path is: C:\temp. The path will be used to store the temporary files generated during the DocAve Agent unattended installation. The temporary files will be deleted as soon as the unattended installation finishes.
-Log	Optional	This is an optional parameter. If used, the logs of the unattended installation will be saved to the .txt file in the specified path. The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Log.txt*. If the specified log file does not exist, it will be generated automatically.
-UseIPv6forCommunication	Optional	This is an optional parameter. It specifies the communication method between the machine where the command is run and the destination machine that the DocAve Agent is installed to. If an IPv6 address is entered in **TargetName** parameter, this parameter must be entered. ***Note**: When using this parameter, both the destination machine and the machine where you run this command must support IPv6.
-ProductType	Required	This parameter is used to identify the product you are installing from other AvePoint's products. Enter *DocAve* as the value of this parameter when you install DocAve products.
-ReceiveInfoPort	Optional	This is an optional parameter to specify a port for the source machine to receive the data from the destination machine. This port and the destination machine's IP are added to an inbound rule of the source machine's firewall so it allows all the connections from the destination machine. DocAve

Parameter	Type	Description
		recommends you configure this parameter to ensure smooth communication between the source machine and the destination machine.
-Timeout	Optional	This is an optional parameter to specify a timeout value for waiting for the return message from the destination machine. A timeout error will occur if there is no message returned from the destination machine in the specified period.
-ReceiveInfoIP	Optional	If multiple IP addresses have been configured on the source machine, use this parameter to specify an IP address for the source machine to communicate with the destination machine.

Getting Configuration Information Command

The **Get-DAAgentConfigInfo** command enables you to remotely get the configuration information of DocAve Agent. You can not only get the configuration information of the Agents installed remotely through the use of Unattended Installation, but also can get the configuration information of the Agents installed locally through the use of installation wizard. In a word, you are able to remotely get the configuration information of any Agents.

Below is an example of the **Get-DAAgentConfigInfo** command:

Get-DAAgentConfigInfo -TargetName *hostmachine* **-Username** *AvePoint\DocAve* **-Password** *"Ave"* **-ProductType** *"DocAve"*

This table contains detailed information for each of the parameters:

Parameter	Type	Description
-TargetName	Required	The name or IP address of the destination machine where has DocAve Agent installed. ***Note**: If the hostname is used, ensure that the specified computer name can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.
-Username	Required	The username of the user used to access the destination machine where has DocAve Agent installed. The format of the username is: domain\username. The permissions of the user specified here are as follows: • If the specified user is the local administrator of the destination machine, it can be used directly.

Parameter	Type	Description
		Enter .*administrator* for the *Username* parameter. • If the specified user is from the domain which the destination machine belongs to, the domain user must be added to the **Administrators** group on the destination machine. The user specified here must have the Full Control permission to the path specified in *RemoteTempPath* parameter.
-Password	Required	The password of the user specified above. Quote the password if it contains any special character or space.
-Log	Optional	This is an optional parameter. If used, the logs of getting configuration information will be saved to the .txt file in the specified path. The generated log file is a text file. The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Log.txt.* If the specified log file does not exist, it will be generated automatically.
-AnswerFilePath	Optional	This is an optional parameter. If used, the configuration information you get by the **Get-DAAgentConfigInfo** command will be exported to the .xml file in the specified path. Only the .xml file is supported by this parameter. The content format of the generated .xml file is the same as the Agent Answer File. The path specified in this parameter must be detailed to the name of the log file. For example, *C:\ManagerConfigInfor.xml.* There must be no .xml file with the same name existing in the specified path.
-ProductType	Required	This parameter is used to identify the product you are installing from other AvePoint's products. Enter *DocAve* as the value of this parameter when you install DocAve products.

Parameter	Type	Description
-UseIPv6forCommunication	Optional	This is an optional parameter used to specify the communication method between the machine where the command is run and the destination machine that the DocAve Agent is installed. If an IPv6 address is entered in **TargetName** parameter, this parameter must be entered. ***Note**: When using this parameter, both the destination machine and the machine where you run this command must support IPv6.
-ReceiveInfoPort	Optional	This is an optional parameter to specify a port for the source machine to receive the data from the destination machine. This port and the destination machine's IP are added to an inbound rule of the source machine's firewall so it allows all the connections from the destination machine. DocAve recommends you configure this parameter to ensure smooth communication between the source machine and the destination machine.
-Timeout	Optional	This is an optional parameter to specify a timeout value for waiting for the return message from the destination machine. A timeout error will occur if there is no message returned from the destination machine in the specified period.
-ReceiveInfoIP	Optional	If multiple IP addresses have been configured on the source machine, use this parameter to specify an IP address for the source machine to communicate with the destination machine.

Configuring Configuration Information Command

The **Config-DAAgentConfigInfo** command enables you to remotely modify the configuration information of DocAve Agent. You can not only modify the configuration information of the Agents installed remotely through the use of Unattended Installation, but also can modify the configuration information of the Agents installed locally through the use of installation wizard. In a word, you are able to remotely modify the configuration information of any Agents.

Below is an example of the **Config-DAAgentConfigInfo** command:

Config-DAAgentConfigInfo *-TargetName hostmachine* **-Username** *AvePoint\DocAve* **-Password** *"Ave"* **-ControlServiceHost** *10.0.0.2* **-ControlServicePort** *15000* **-AgentAddress** *10.0.0.1*

This table contains detailed information for each of the parameters:

Parameter	Type	Description
-TargetName	Required	The name or IP address of the destination machine where has DocAve Agent installed.

Parameter	Type	Description
		***Note**: If the hostname is used, ensure that the specified computer name can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.
-Username	Required	The username of the user used to access the destination machine where has DocAve Agent installed. The format of the username is: domain\username. The permissions of the user specified here are as follows: • If the specified user is the local administrator of the destination machine, it can be used directly. Enter .*administrator* for the *Username* parameter. • If the specified user is from the domain which the destination machine belongs to, the domain user must be added to the **Administrators** group on the destination machine. The user specified here must have the Full Control permission to the path specified in *RemoteTempPath* parameter.
-Password	Required	The password of the user specified above. Quote the password if it contains any special character or space.
-ControlServiceHost	Optional	If the host name or IP address of the Control service that connects the Agent installed on the destination machine is changed, use this parameter to change the host name or IP address of the Control service to the new one.
-ControlServicePort	Optional	If the port of the Control service that connects the Agent installed on the destination machine is changed, use this parameter to change the port of the Control service to the new one.
-AgentHost	Optional	If the host name or IP address of the destination server that has Agent installed is changed, use this parameter to change the host name or IP address of the Agent to the new one.
-AgentPort	Optional	The new Agent port you want to use for the DocAve Agent installed on the destination machine.

Parameter	Type	Description
-Passphrase	Required	The passphrase for the Control service that you want to use for the DocAve Agent installed on the destination machine.
-Log	Optional	This is an optional parameter. If used, the logs of configuring configuration information will be saved to the .txt file in the specified path. The generated log file is a text file. The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Log.txt.* If the specified log file does not exist, it will be generated automatically.
-ProductType	Required	This parameter is used to identify the product you are installing from other AvePoint's products. Enter *DocAve* as the value of this parameter when you install DocAve products.
-UseIPv6forCommunication	Optional	This is an optional parameter used to specify the communication method between the machine where the command is run and the destination machine that the DocAve Agent is installed. If an IPv6 address is entered in **TargetName** parameter, this parameter must be entered. ***Note**: When using this parameter, both the destination machine and the machine where you run this command must support IPv6.
-ReceiveInfoPort	Optional	This is an optional parameter to specify a port for the source machine to receive the data from the destination machine. This port and the destination machine's IP are added to an inbound rule of the source machine's firewall so it allows all the connections from the destination machine. DocAve recommends you configure this parameter to ensure smooth communication between the source machine and the destination machine.
-Timeout	Optional	This is an optional parameter to specify a timeout value for waiting for the return message from the destination machine. A timeout error will occur if there is no message returned from the destination machine in the specified period.

Verifying Configuration Information Command

The **Verify-DAAgentConfigInfo** command enables you to remotely verify the configuration information you want to use for DocAve Agent is valid or not. You can not only verify the configuration information for the Agents installed remotely through the use of Unattended Installation, but also can modify the configuration information for the Agents installed locally through the use of installation wizard. In a word, you are able to remotely verify the configuration information for any Agents.

Below is an example of the **Verify-DAAgentConfigInfo** command:

Verify -DAAgentConfigInfo *-TargetName hostmachine* **-Username** *AvePoint\DocAve* **-Password** *"Ave"* **-ControlServiceHost** *10.0.0.2* **-ControlServicePort** *15000* **-AgentAddress** *10.0.0.1*

This table contains detailed information for each of the parameters:

Parameter	Type	Description
-TargetName	Required	The name or IP address of the destination machine where has DocAve Agent installed. ***Note**: If the hostname is used, ensure that the specified computer name can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.
-Username	Required	The username of the user used to access the destination machine where has DocAve Agent installed. The format of the username is: domain\username. The permissions of the user specified here are as follows: • If the specified user is the local administrator of the destination machine, it can be used directly. Enter *.\administrator* for the *Username* parameter. • If the specified user is from the domain which the destination machine belongs to, the domain user must be added to the **Administrators** group on the destination machine. The user specified here must have the Full Control permission to the path specified in *RemoteTempPath* parameter.

Parameter	Type	Description
-Password	Required	The password of the user specified above. Quote the password if it contains any special character or space.
-ControlServiceHost	Optional	Verifying the host name or IP address of the Control service that you want the Agent installed on the destination machine to connect.
-ControlServicePort	Optional	Verifying the port of the Control service that you want the Agent installed on the destination machine to connect.
-AgentHost	Optional	Verifying the host name or IP address that you want to use for the Agent installed on the destination machine.
-AgentPort	Optional	Verifying the port that you want to use for the Agent installed on the destination machine.
-Passphrase	Required	The passphrase for the Control service that you want to use for the DocAve Agent installed on the destination machine.
-Log	Optional	This is an optional parameter. If used, the logs of verifying configuration information will be saved to the .txt file in the specified path. The generated log file is a text file. The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Log.txt.* If the specified log file does not exist, it will be generated automatically.
-ProductType	Required	This parameter is used to identify the product you are installing from other AvePoint's products. Enter *DocAve* as the value of this parameter when you install DocAve products.
-UseIPv6forCommunication	Optional	This is an optional parameter used to specify the communication method between the machine where the command is run and the destination machine that the DocAve Agent is installed. If an IPv6 address is entered in **TargetName** parameter, this parameter must be entered.

Parameter	Type	Description
		***Note**: When using this parameter, both the destination machine and the machine where you run this command must support IPv6.
-ReceiveInfoPort	Optional	This is an optional parameter to specify a port for the source machine to receive the data from the destination machine. This port and the destination machine's IP are added to an inbound rule of the source machine's firewall so it allows all the connections from the destination machine. DocAve recommends you configure this parameter to ensure smooth communication between the source machine and the destination machine.
-Timeout	Optional	This is an optional parameter to specify a timeout value for waiting for the return message from the destination machine. A timeout error will occur if there is no message returned from the destination machine in the specified period.
-ReceiveInfoIP	Optional	If multiple IP addresses have been configured on the source machine, use this parameter to specify an IP address for the source machine to communicate with the destination machine.

Getting Help Information About DocAve Agent Unattended Installation Commands

Once you have imported the UnattendedInstallation.dll file, you can user the **Get-Help** command to get help information about any of the above DocAve Agent Unattended Installation commands. This command enables you to get comprehensive information for the specified command, including the syntax, description, detailed information for each parameter**,** and examples.

For example, if you want to get the help information of the **Install-DAAgent** command, enter the following command:

Get-Help *Install-DAAgent* **–Full**

Helpful Notes for DocAve Unattended Installation to Windows XP Operating System

Connecting to the remote environment with the Windows XP operating system is refused when executing DocAve unattended installation. The solution strategy to this issue is:

Navigate to the remote server where you want to perform the unattended installation, and set the configurations according to the steps below:

1. Navigate to **Start > Control Panel > Administrative Tools**.
2. Click **Local Security Policy** to access to the Local Security Settings interface .
3. Expand the **Local Policies** node, and select **Security Options**.
4. Select **Network access: Sharing and security model for local accounts**. Set its value as **Classic- local users authenticate as themselves**.

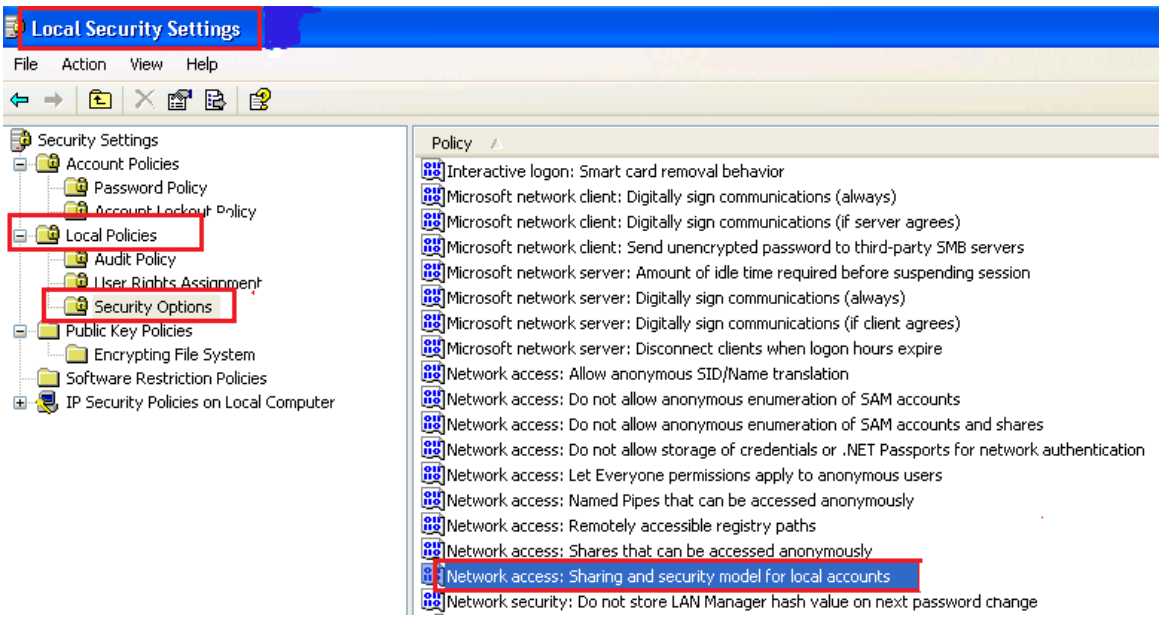


Figure 1: The Local Security Settings interface.

After the configuration above, you can try to remotely run the unattended installation job on the environment with Windows XP operating system.

Accessing the DocAve GUI

The following table provides the required browser versions and the required Silverlight version if you want to access DocAve GUI in Windows Server 2008 R2 Enterprise SP1 environment.

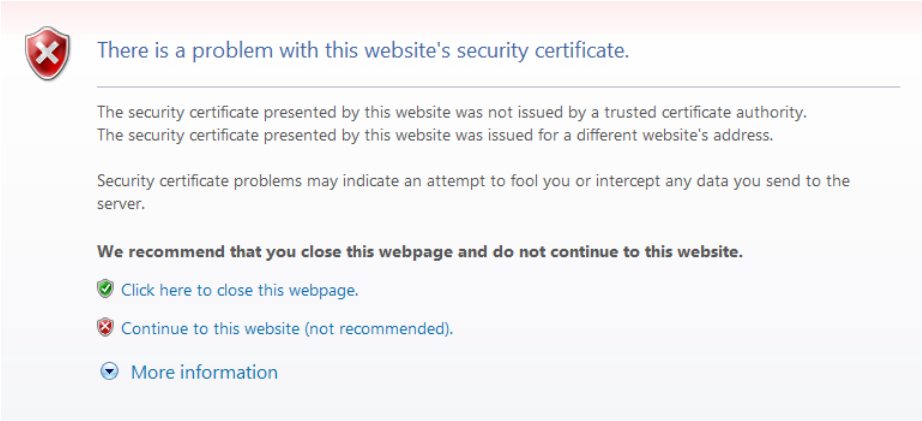
Rules	Requirements
Silverlight Version	5.0 or above
Internet Explorer	IE 7 or above
Google Chrome	19.0.1084.52
Mozilla Firefox	14.0.1

DocAve 6 is able to be installed and accessed in the environment that has been configured according to the USGCB (United States Government Configuration Baseline) security standards. Please visit the website http://usgcb.nist.gov/usgcb/microsoft_content.html to get more information on USGCB.

Internet Explorer Setup

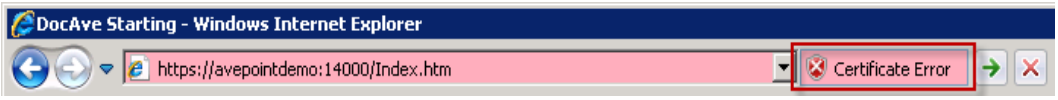
When first accessing DocAve using Microsoft Internet Explorer (IE), certain initial security settings must be configured. Run DocAve's server application found in the start menu on the machine running the DocAve Control service, and complete the following steps:

1. When you access DocAve by IE, the Browser will display a security certificate prompt:

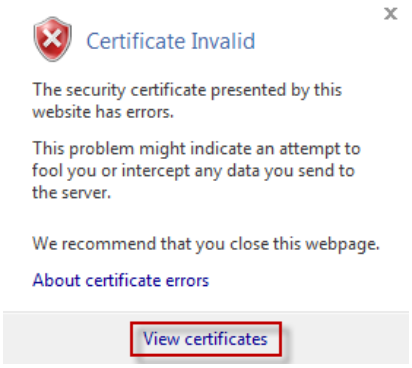


   Select the option **Continue to this website** listed by the red bullet.

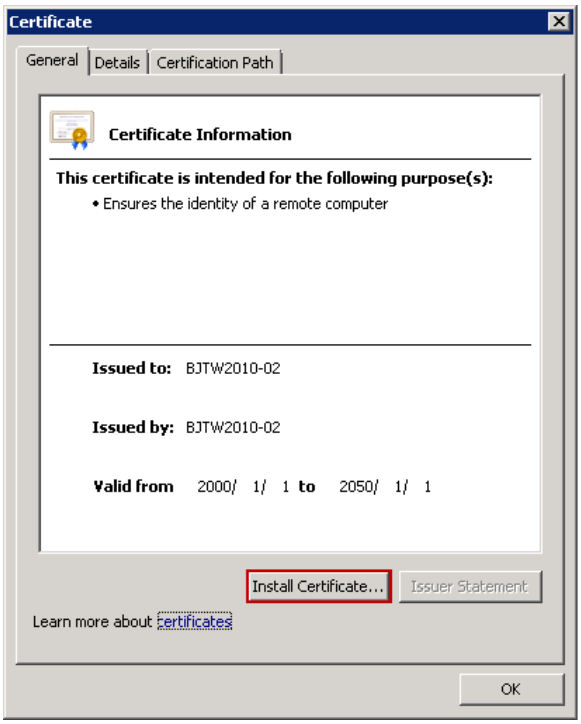
2. Click the **Security Report** icon next to the address URL.



3. Click **View certificates** in the pop-up. The Certificate window appears.

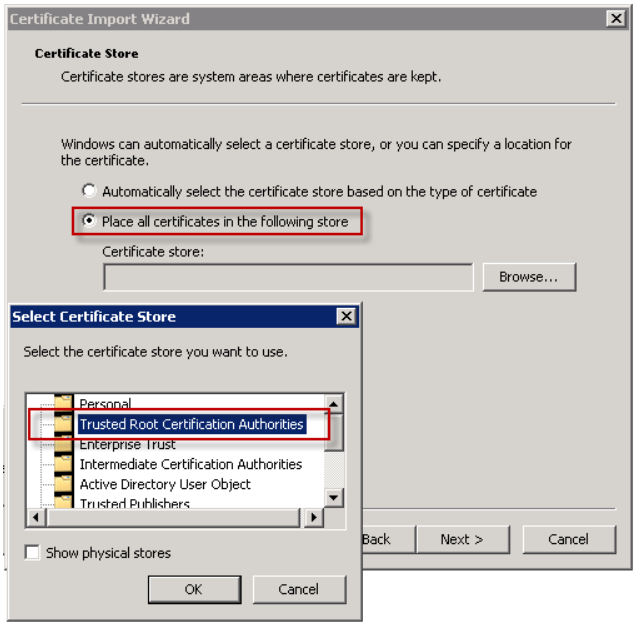


4. Click **Install Certificate…** button to install DocAve certificate. The name of this certificate is the same as the hostname of the server that has DocAve Control service installed.

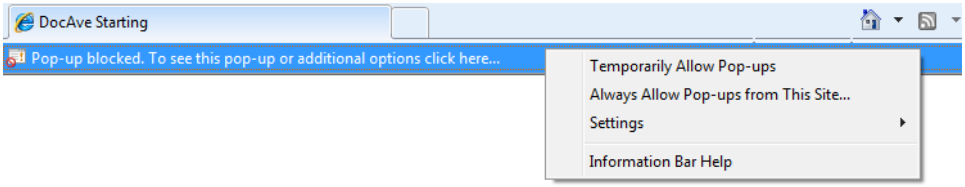


5. Click **Next** to continue with the Certificate Import.

6. Select the **Place all certificates in the following store** option and click **Browse** to browse to **Trusted Root Certification Authorities** folder. Click **OK** to confirm the selection and click **Next**.



7. Click **Finish** to complete the certificate import.
8. Click **OK** in the prompt acknowledging the successful import.
9. Select temporarily allow popping up the DocAve GUI or always allow in the security prompt.



Now you can log into DocAve from Internet Explorer.

Logging into DocAve

The DocAve GUI can be launched from web browsers within the same network as the DocAve Manager. Refer to Accessing the DocAve GUI for the supported web browsers. Connect to the interface using the IP/Hostname for the DocAve Manager - Control service, as well as the Control Service Port if it was changed.

1. Open an Internet Explorer window and enter: *https://<machine>:14000*.

   Where <machine> is the hostname or IP address of the machine running the DocAve Control service. If the default port number has been changed from 14000, enter the new port number.

***Note**: If the hostname of the machine running the DocAve Control service contains the *underline* (_), use the IP address of the corresponding machine to access DocAve.

2. The DocAve login screen pops up. Select Local System and enter the default login account information:

   - Login ID: admin
   - Password: admin

   Click **Login**.

   ***Note**: When you log on DocAve for the first time, it is strongly recommended backing up the DocAve security keys for protection. For more information, refer to the DocAve 6 Control Panel Reference Guide.

You can also log on DocAve using the integration with other authentication methods. For more information, refer to the DocAve 6 Control Panel Reference Guide.

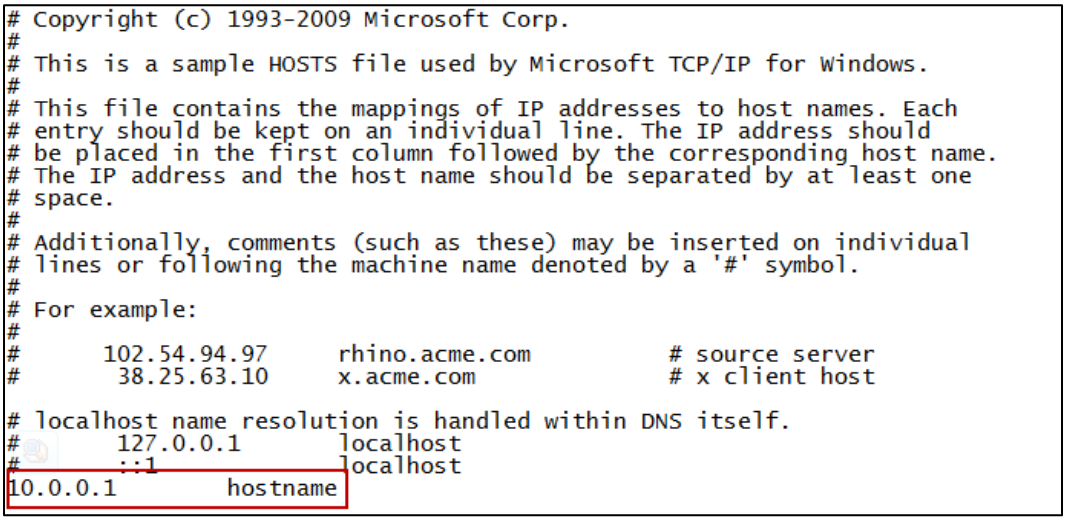
Out-of-Browser Accessing DocAve Manager

DocAve Manager can be installed as a shortcut on the local machine when remotely accessing the DocAve Manager, allowing you to double-click the shortcut rather than using the URL.

Follow the instructions below to perform Out-of-Browser (OOB) installation.

1. On the machine where you want to perform OOB installation, add a mapping for the IP address of the machine where your DocAve Manager is installed.

   For example, if you use the DocAve build-in certificate which uses the same name as the hostname of the machine where the DocAve Manager is installed, add the mapping according to the following figure:



***Note**: If your DocAve 6 is updated from DocAve 6 GA, you must add the mapping for the IP address of the machine where your DocAve Manager installed.

2. Use the URL with the certificate to access DocAve Manager:

   https://hostname:14000/Index.htm

   ***Note**: If your DocAve 6 is updated from DocAve 6 GA, the URL with the mapped certificate is as follows:

   https://docave:14000/Index.htm

   Since the DocAve build-in certificate is not CA-certified, you must install it to access DocAve Manager. Refer to Internet Explorer Setup for more information on installing the DocAve certificate.

3. After the DocAve certificate is installed successfully, login DocAve Manager and right-click on DocAve Manager GUI. Select **Install DocAve 6 onto this computer…**
4. Click **Install** in the pop-up window to install the DocAve Manager shortcut on the desktop of the local machine. Now you can remotely access DocAve Manager by double-clicking the shortcut rather than using the URL.

DocAve Manager and Agent Maintenance

Using the DocAve Manager/Agent Configuration Tool

If you want to modify the configuration of DocAve Manager/Agent after the installation, open the **Start Menu** in Windows on the DocAve Manager server, and navigate to **All Programs** > **AvePoint DocAve 6**. Then open the **DocAve 6 Manager Tools**/**DocAve 6 Agent Tools** folder. Click **Manager Configuration Tool**/**Agent Configuration Tool**.

Click on the items listed on the left part of the tool and you can modify the corresponding settings.

Refer to Installing DocAve Manager and Installing DocAve Agent for the detailed information of the settings.

***Note**: If the database type is MS SQL, you can change the Control database/Auditor database/Report database to another existing Control database/Auditor database/Report database using DocAve Manager Configuration Tool. Moreover, the passphrase is required to be entered if you choose to change the Control database to another existing Control database. The Manager Configuration Tool does not support the data transformation. If you want to use the data in the former database, it is recommended that you back up the data to the server (you wish to use), and connect the specified server with the transferred database using the Manager Configuration Tool.

Using the DocAve Manager/Agent Restart Service Tool

If you want to restart the services of DocAve Manager/Agent after the installation, open the **Start Menu** in Windows on the DocAve Manager server and navigate to **All Programs** > **AvePoint DocAve 6**. Then open the **DocAve 6 Manager Tools**/**DocAve 6 Agent Tools** folder. Click **Manager Restart Service Tool**/**Agent Restart Service Tool**.

You can check the status of the services in the tool interface. Select one service from the tool interface and you can perform the following actions.

- **Start** – Start the selected services which have been stopped.
- **Stop** – Stop the selected services.
- **Restart** – Restart the selected services.

Using the DocAve Manager/Agent Uninstallation Wizard

You can use either of the two methods below to access the uninstallation wizard of DocAve Manager/Agent after the Manager/Agent has been installed. In order to complete the change/repair operations successfully, the Uninstallation Wizard must be run by a local administrator.

- Method 1 – Double click the *Setup.exe* file in the unpacked DocAve Manager/Agent directory and run it.

  ***Note**: This is the recommended method since it makes the most use of the installation package.

- Method 2 – Open the Start Menu in Windows on the DocAve Manager/Agent server and navigate to *All Programs > AvePoint DocAve 6*. Open **DocAve 6 Manager Tools**/**DocAve 6 Agent Tools** folder. Click **Manager Uninstall**/**Agent Uninstall**.

Now you can perform the operations introduced in the following two sections.

Change the Manager Installation

You can install/uninstall the specified Manager services by selecting the **Change** option in the DocAve Manager uninstallation wizard. This option is very useful when you want to add new services onto the server or remove existing services from the server.

After the **Installation Rule Scanning**, you will then be guided through the installation/uninstallation of the selected Manager services.

Repair the Manager/Agent Installation

You can try to repair the DocAve Manager/Agent files after they have been corrupted.

Select the **Repair** option in the DocAve Manager/Agent uninstallation wizard, and DocAve will try to repair the corrupted files.

However, there are some limitations to the **Repair** function:

- If some crucial files are missing or corrupted, the DocAve installation cannot be repaired.
- If you have cleared the temporary files after the first installation, or the version of the Data.cab file is not the same as the version of the current platform, you must select a valid repairing file with the same version as the version of your current platform for the repair using **Manager Uninstall**/**Agent Uninstall** wizard. The repairing file can be the Data.cab file or an update. You can also perform the repair using the **Setup.exe** file in the unpacked DocAve Manager/Agent directory.
- If the register key HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Uninstall > DocAve6Manager or key HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Uninstall > DocAve6Agent is corrupt, you must select a valid repairing file with the same version as the version of your current platform for the repair using Manager Uninstall/Agent Uninstall wizard. The repairing file can be the Data.cab file or an update. You can also use the Setup.exe file in the unpacked DocAve Manager/Agent directory to perform a new installation of DocAve.

Uninstalling DocAve

The DocAve Uninstallation Wizard is there to guide you through this uninstallation process. By following the steps below, you will have DocAve removed from your environment very quickly. In order to complete the uninstallation successfully, the Uninstallation Wizard must be run by a local administrator.

Uninstalling DocAve Software

Before uninstalling DocAve, there are additional steps needed to restore your content back to SharePoint. If the Storage Optimization product was used, complete the following steps before uninstalling DocAve Manger and Agent.

Storage Manager

To uninstall Storage Manager, complete the following steps:

1. Disable any relevant rules. For more information on disabling rules, refer to the **Enabling and Disabling Rules** section in the Storage Manager User Guide.
2. Perform a **Convert Stub to Content** job. This will restore your content. For more information, refer to the **Converting Stubs to Content** section in the Storage Manager User Guide.

Archiver

To uninstall Archiver, you will need to perform an **In Place Restore** to restore the archived data back to SharePoint. For more information, refer to the **Restoring Archiver Data** section in the Archiver User Guide.

Connector

The options for uninstalling Connector will differ according to the library type: SharePoint Built-in Libraries or Connector Libraries. Complete the steps below based on your library type:

- **SharePoint Built-in Libraries**
    - Keep content in SharePoint – Perform a **Convert Stub to Content** job and then delete **Connector Settings** in the corresponding library settings. For more information, refer to the **Converting Stubs to Content** and **Removing Connector Settings** sections in the Connector User Guide.
    - Don't keep content in SharePoint – Delete the **Connector Settings** in the corresponding library. This will delete the stubs in the library. For more information, refer to the **Removing Connector Settings** section in the Connector User Guide.

- **Connector Libraries**
    - Keep content in SharePoint – Once the Connector solutions are uninstalled, this library will not be accessible.
    - Don't keep content in SharePoint – Delete the **Connector libraries**. For more information, refer to the **Removing Connector Settings** section in the Connector User Guide.

After removing your libraries, uninstall the Connector solutions. To uninstall Connector solutions, you will need to retract the deployment of the farm solution's components. To do so,

1. Navigate to **Control Panel > Solution Manager**.
2. Select the applicable solutions.
3. Click **Retract** from the Actions group on the ribbon.

For more information on retracting solutions, refer to the **Operations on the Solutions** section in the Control Panel User Guide.

***Note:** The content will still exist in the storage after the library is deleted.

Uninstalling DocAve Manager

In order to uninstall DocAve Manager, please ensure the manager service being removed is not in use by another process.

Uninstalling DocAve Manager from Common Environments

If your DocAve Manager is installed on the following common Windows environments:

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows 7
- Windows 8
- Windows Server 2012
- Windows Server 2012 R2

To uninstall DocAve Manager, complete the following steps:

1. Open the **Start Menu** in Windows on the DocAve Manager server, and navigate to **All Programs** > **AvePoint DocAve 6**.
2. Open DocAve 6 Manager Tools folder. Click Manager Uninstall.

3. Select the **Remove** option. Click **Next**.
4. In Ready to Remove DocAve 6 Manager page, configure the following option.
    - **Remove configuration file** – Select this option if you want to remove all the folders and configuration files generated by the DocAve 6 Manager installation.

      ***Note:** The Logs folder will not be removed no matter you select **Remove configuration file** option or not. If you will want to use the Control database later, you first back up the passphrase by going to **Control Panel** > **System Option** > **Security Information** > **Manager Passphrase**.

    Click **Remove** to start the Manager uninstallation process.

    ***Note**: Removing DocAve Manager will make the currently running jobs failed.

    If the application pool created by DocAve Manager installation is still useful, it will not be deleted during the Manager uninstallation. If the application pool created by DocAve Manager installation is not used by any other applications, it will be deleted during the Manager uninstallation.

    If you use Built-in database, you will be asked whether to delete the Built-in database while uninstalling DocAve Manager. If you use SQL Server, the Manager uninstallation will not delete the Manager databases.
5. Click **Finish** to complete the uninstallation.

***Note:** Once the uninstallation is in progress, it cannot be cancelled and the uninstallation interface cannot be closed.

Uninstalling DocAve Manager from Windows Server Core Environments

Follow the steps below to uninstall DocAve Manager from Windows Server 2008 R2 SP1 Server Core environment.

1. Change the directory to the unzipped DocAve Manager installation package in Command Line interface.
2. Enter the following command and press **Enter** to start the DocAve Manager uninstallation process.

    Setup.exe Uninstall-DocAveManager -RemoveConfigurationFile

    The parameter **-RemoveConfigurationFile** is optional. If you add the remove configure file parameter after the command, all the folders and the configuration files generated by DocAve Manager installation will be removed after the uninstallation completes.

    ***Note:** Remove configuration file does not remove the Logs folder.

***Note:** If the application pool created by DocAve Manager installation is not used by any other applications, it will be deleted during the Manager uninstallation.

***Note:** The Manager uninstallation will not delete the Manager databases from SQL Server.

Uninstalling DocAve Agent

In order to uninstall DocAve Agent, please ensure there are no current jobs running on the agent.

Uninstalling DocAve Agent from Common Environments

If your DocAve Agent is installed on the following common Windows environments:

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows Server 2012

To uninstall DocAve Agent, complete the following steps:

1. Open the **Start Menu** in Windows on the DocAve Agent server, and navigate to **All Programs** > **AvePoint DocAve 6.**
2. Open DocAve 6 Agent Tools folder. Click Agent Uninstall.
3. Select the **Remove** option. Click **Next**.
4. In Ready to Remove DocAve 6 Agent page, configure the following options.
    - **Disable EBS/RBS settings in SharePoint farm** – Select this option to disable the EBS/RBS settings in the SharePoint farm. If the EBS/RBS settings are disabled, the Storage Optimization stubs cannot be accessed. This option is selected by default. Uncheck this option if you want to reinstall the DocAve 6 Agent later.
    - **Remove configuration file** – Select this option if you want to remove all the folders and configuration files generated by the DocAve 6 Agent installation.

      ***Note**: The Logs folder will not be removed no matter you select **Remove configuration file** option or not.

Click **Remove** and the Agent uninstallation process starts.

*__Note__: Removing DocAve Agent will fail the currently running jobs and stop the currently running processes. Click **View Details** in the pop-up window to view the detailed information about the running jobs and processes.

5. Click **Finish** to complete the uninstallation.

***Note:** Once the uninstallation is in progress, it cannot be cancelled and the uninstallation interface cannot be closed.

Uninstalling DocAve Agent from Windows Server Core Environments

To uninstall DocAve Agent from Windows Server 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core environment, complete the following steps:

1. Change the directory to the unzipped DocAve Agent installation package in Command Line interface.
2. Enter the following command and press Enter to start the DocAve Agent uninstallation process:

   Setup.exe Uninstall-DocAveAgent -RemoveConfigurationFile -IsCheckDisableEBSRBS

3. **-RemoveConfigurationFile** and **-IsCheckDisableEBSRBS** are optional parameters.
   - If you only use the command without any parameter appended, the EBS/RBS settings in the SharePoint farm are disabled, and the Storage Optimization stubs cannot be accessed. Also all the folders and configuration files generated by the DocAve 6 Agent installation will not be removed after the uninstallation completes.
   - Adding the parameter**-RemoveConfigurationFile** after the command, all the folders and configuration files generated by the DocAve 6 Agent installation will be removed after the uninstallation completes.
   - Adding the parameter **-IsCheckDisableEBSRBS** after the command, the EBS/RBS settings in the SharePoint farm are not disabled during the uninstallation.

Advanced Configuration

For advanced configuration, you are able to modify the ports used by DocAve Storage Manager, Connector, and Replicator.

Modify the Port Used by DocAve Storage Manager and Connector

On a specified DocAve Agent server, if the default port (14005) used by DocAve Storage Manager and Connector is occupied, you can use the following configuration file to modify the port:

…\AvePoint\DocAve6\Agent\data\SP2010\Arch\AgentCommonStorageEnv.cfg

To modify the port used by DocAve Storage Manager and Connector, complete the following steps:

1. Navigate to the installation path of the specified DocAve Agent, which is *…\AvePoint\DocAve6\Agent\data\SP2010\Arch* by default.
2. Find the **AgentCommonStorageEnv.cfg** file and open it with Notepad.
3. Modify the value of **StorageServicePort** to an available port.
4. Save the configuration file.
5. Click **Start** and find the Command Prompt.
6. Right click on it and click **Run as administrator**.
7. Enter **iisreset** in the popup Command Prompt, and press **Enter** to restart IIS.
8. Restart the DocAve Agent service. For more information, refer to Using the DocAve Manager/Agent Restart Service Tool section.

Modify the Port Used by DocAve Replicator

On a specified DocAve Agent server, if the default port (14006) used by DocAve Replicator is occupied, you can use the following configuration file to modify the port:

…\AvePoint\DocAve6\Agent\data\SP2010\Replicator\SP2010Replicator.xml

To modify the port used by DocAve Replicator, complete the following steps:

1. Navigate to the installation path of the specified DocAve Agent, which is *…\AvePoint\DocAve6\Agent\data\SP2010\Replicator* by default.
2. Find the *SP2010Replicator.xml* file, and open it with Notepad.
3. Modify the value of **ListenerPort** to an available port.
4. Save the configuration file.

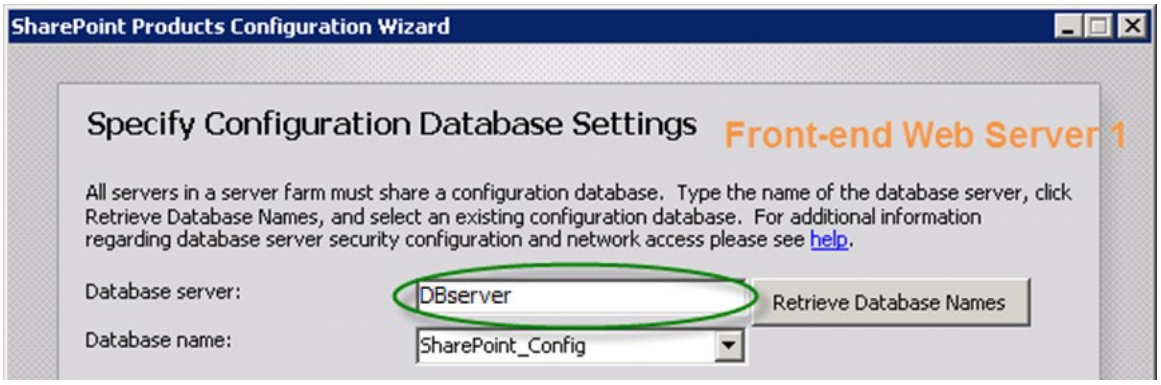
5. Click **Start,** and find the Command Prompt.
6. Right click on it and click **Run as administrator**.
7. Enter **iisreset** in the pop-up Command Prompt and press **Enter** to restart IIS.
8. Restart the DocAve Agent service. For more information, refer to Using the DocAve Manager/Agent Restart Service Tool section.

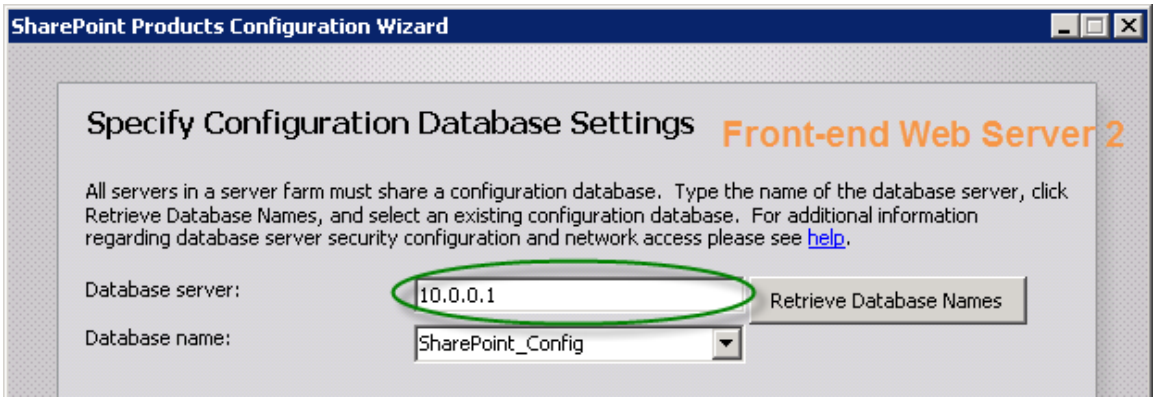
Helpful Notes

The following sections provide some helpful notes concerning issues displaying DocAve Agents in the Manager interface, collation issues, and how to get additional help for any additional issues you have during installation.

Installed DocAve Agents Cannot be Displayed in the Manager Interface

If both hostname and IP address are used to configure the **Database server** when installing SharePoint on the Web front-end servers, the DocAve agents installed on the Web front-end servers may not be displayed in **DocAve 6** > **Control Panel** > **System Settings** > **Monitor** > **Agent Monitor**.





After the DocAve Agents have been installed on the Web front-end servers successfully, refer to the following steps to resolve this issue:

1. Remotely log on one Agent server which is displayed correctly in the Manager Interface.
2. Navigate to the installation path of DocAve Agent, by default it is **C:\Program Files\AvePoint\DocAve6\Agent\bin**.
3. Find the configuration file named **AgentCommonVCEnv.config**.

4. Copy the **AgentCommonVCEnv.config** file and save it to a local path.
5. Remotely log on each of the Agent servers which cannot be displayed in the Manager Interface.
6. Navigate to the installation path of DocAve Agent, by default it is **C:\Program Files\AvePoint\DocAve6\Agent\bin**.
7. Find the configuration file named **AgentCommonVCEnv.config**.
8. Open it with Notepad, and find the following two nodes.

   <**add key**="**agentFarmName**" **value**="*Farm(DocAveVM:SHAREPOINT_CONFIG)*" />

   <**add key**="**agentFarmId**" **value**="226e10b4-2801-43da-b2ab-1c8b350bc4b8" />

   Modify the values of **agentFarmName** and **agentFarmId** according to the *AgentCommonVCEnv.config* file obtained in Step 4.
9. Save the modification and restart the DocAve 6 Agent service. Refer to Using the DocAve Manager/Agent Restart Service Tool for the detailed steps of restarting the DocAve 6 Agent service.
10. Navigate to **DocAve 6** > **Control Panel** > **System Settings** > **Monitor** > **Agent Monitor**, and set the Agent Account of the Agents mentioned in Step 5. For more information on configuring the Agent Account, refer to the Control Panel user guide.
11. Save the modification and restart the DocAve 6 Agent service. Refer to Using the DocAve Manager/Agent Restart Service Tool for the detailed steps of restarting the DocAve 6 Agent service.

The issue will be resolved.

Database Collation Issue

If you encounter a database collation error when using an existing database that is not a DocAve database during the DocAve Manager installation process, log into SQL, and configure the following settings according to the following steps:

1. Log into SQL, and choose the specified database that you wish to use.
2. Right-click the specified database, and then select **Properties**.
3. Select **Options** and set **Latin1_General_CI_AS_KS_WS** for the corresponding collation of the specified database.

After the configuration above, to successfully use an existing database that is not a DocAve created database, you must guarantee that the database is empty.

Other Issues

If you encounter other issues when installing the DocAve Manager or Agents, follow the prompt messages to resolve the issue, and run the installation program again. If the issue persists, refer to the AvePoint Technical Support site for additional help.

Appendix A: Where to Install DocAve Agents

Refer to the following table for the detailed places to install DocAve Agents in order to use each product of the DocAve platform. The specified places to install DocAve Agents are the basic requirements to make all of the functions and configurations of each product available. All of the installed DocAve Agents must be proper licensed in the modules and functions you want to use.

Product Suites	Product		Detailed Places to Install DocAve Agents
Migration	SharePoint 2007 to 2010 Migration	Source: SharePoint 2007	DocAve Agent must be installed on at least one of the source Web front-end servers.
		Destination: SharePoint 2010	DocAve Agent must be installed on at least one of the destination Web front-end servers.
	SharePoint 2007 to 2013 Migration	Source: SharePoint 2007	DocAve Agent must be installed on at least one of the source Web front-end servers.
		Destination: SharePoint 2013	DocAve Agent must be installed on at least one of the destination Web front-end servers.
	SharePoint 2010 to 2013 Migration	Source: SharePoint 2010	DocAve Agent must be installed on at least one of the source Web front-end servers.
		Destination: SharePoint 2013	DocAve Agent must be installed on at least one of the destination Web front-end servers.
	Lotus Notes Migration	Source: Lotus Notes	DocAve Agent must be installed on the server with Lotus Notes Client installed.
		Destination: SharePoint 2010 SharePoint 2013	DocAve Agent must be installed on the Web front-end servers where you want to perform migration.
	Quickr Migration	Source: Quickr	DocAve Agent must be installed on the server with Lotus Notes Client, Domino Server, and Quickr (QuickPlace) installed.
		Destination: SharePoint 2010 SharePoint 2013	DocAve Agent must be installed on the Web front-end servers where you want to perform migration.
	File System Migration	Source: File System	DocAve Agent must be installed on at least one of the File System servers with Windows XP Operating System or above.

Product Suites	Product		Detailed Places to Install DocAve Agents
		Destination: SharePoint 2010 SharePoint 2013	DocAve Agent must be installed on the Web front-end servers where you want to perform migration.
	Livelink Migration	Source: Livelink	DocAve Agent must be installed on at least one of the servers which can connect to the Livelink server and has the following components installed: • .Net Framework 3.5.1 • Microsoft Visual J# Version 2.0
		Destination: SharePoint 2010 SharePoint 2013	DocAve Agent must be installed on the Web front-end servers where you want to perform migration.
	eRoom Migration	Source: eRoom	DocAve Agent must be installed on the eRoom server.
		Destination: SharePoint 2010 SharePoint 2013	DocAve Agent must be installed on the Web front-end servers where you want to perform migration.
	Exchange Public Folder Migration	Source: Exchange Public Folder	DocAve Agent must be installed on at least one of the servers which are able to access the server with Exchange installed. If the MAPI access method is used in the Exchange Public Folder connection, DocAve Agent must be installed on the server with Microsoft Outlook installed and the server must be able to access the server with Exchange installed. If destination Web front-end servers are able to access the server with Exchange installed, you can use the same Agent installed on Web front-end servers for both source and destination.
		Destination: SharePoint 2010 SharePoint 2013	DocAve Agent must be installed on the Web front-end servers where you want to perform migration.
	EMC Documentum Migration	Source: EMC Documentum	DocAve Agent must be installed on the EMC Documentum server or the machine that

Product Suites	Product		Detailed Places to Install DocAve Agents
			install the **Documentum DFC Runtime Environment** program.
		Destination: SharePoint 2010 SharePoint 2013	DocAve Agent must be installed on the Web front-end servers where you want to perform migration.
Data Protection	Granular Backup & Restore		DocAve Agent must be installed on at least one of the Web front-end servers.
	Platform Backup & Restore		DocAve Agent must be installed on the following servers: • DocAve Agent must be installed on at least one of the Web front-end servers. • The Search Service Application server where you want to back up the components of the specified Search Service Application. • The SharePoint Foundation (Help) Search server where you want to back up the components of the SharePoint Foundation (Help) Search. • Each SharePoint server where you want to back up the following objects: IIS Settings, SharePoint Hive, Global Assembly Cache, Custom Features, SharePoint Site Definitions and Extra File System Folders. • Each FAST Search server where you want to back up the FAST Search server settings. • The server with Microsoft SQL Server installed. • Each node of Microsoft SQL Cluster. ***Note**: Platform Backup supports SQL clustering, but only MSCS is supported. Failover is not supported for a third party cluster, but there is a manual workaround. If cluster failover support is required, install the DocAve Agent on each SQL cluster node. If it is not required, the DocAve Agent only needs to be installed on the active nodes. When configuring the DocAve Agent, make sure the **Agent Name**

Product Suites	Product		Detailed Places to Install DocAve Agents
			field matches the cluster virtual node name. • Each replica of the Microsoft SQL **AlwaysOn Availability Groups** if you are using SQL Server 2012 • The source SQL server and the failover SQL server on the SQL mirroring database where you want to perform the Platform Backup and Restore job. • To perform a Farm Rebuild, install DocAve Agent on each server in the SharePoint farm (including all of the SharePoint servers and SQL servers).
	SQL Server Data Manager	Analyze SQL Server Data	DocAve Agent must be installed on a SQL Server.
		Restore SQL Server Data	DocAve Agent must be installed on a SharePoint server with the Microsoft SharePoint Foundation Web Application service started.
	High Availability		DocAve Agent must be installed on the following servers: • Install the DocAve Agent on all of the SharePoint servers in the SharePoint farms to make sure that the High Availability Failover and Fallback job can be performed in any High Availability Mode or Failover Method. • All of the SQL servers where the SharePoint databases reside. ***Note**: If the version of the SQL Server used by your SharePoint 2013 farm is SQL Server 2008 R2, you must install the .NET Framework 4.5 on this SQL Server. • Each node of Microsoft SQL Cluster. • Each replica of the **AlwaysOn Availability Group** where you will perform the High Availability jobs with **AlwaysOn Availability Group** method. ***Note**: DocAve recommends installing the DocAve Agent on each replica of the Microsoft SQL **AlwaysOn Availability Groups**, if you are using SQL Server 2012.
Administration	Administrator		DocAve Agent must be installed on at least one of the Web front-end servers.
	Content Manager		

Product Suites	Product	Detailed Places to Install DocAve Agents
	Deployment Manager	***Note**: For Deployment Manager, if you want to run the Metadata Service Rollback job or the Metadata Service Backup job, DocAve Agent must be installed on the corresponding SQL server.
	Replicator	DocAve Agent must be installed on at least one of the Front-end Web servers. ***Note**: If you want to use Real-Time Replication, DocAve Agents must be installed on all the Web front- end servers.
Compliance	eDiscovery	• DocAve Agent must be installed on at least one of the Web front-end servers. • DocAve Agent must be installed on the server with Search Service started.
	Vault	DocAve Agent must be installed on at least one of the Web front-end servers.
Report Center		DocAve Agents must be installed on all the Web front-end servers. ***Note**: If you want to use the Cross-Farm Service Configuration functions, you must install DocAve agent on the server with SharePoint Central Administration installed.
Storage Optimization	Real-Time/Scheduled Storage Manager(In RBS environment)	• DocAve Agents must be installed on all the Web front-end servers. • DocAve Agent must be installed on the server which installs the Office Web App service. Office Web App service includes Word Viewing Service Application, PowerPoint Service Application and Excel Calculation Services. • If you installed the **Microsoft SQL Server Reporting Services Add-in** for Microsoft SharePoint technologies, and generated stubs for the **Report Builder Model**, you must install DocAve Agent on the server which installs the add-in.
	Real-Time/Scheduled Storage Manager(In EBS environment)	• DocAve Agents must be installed on the SharePoint Central Administration server and all the Front-end Web servers. • DocAve Agent must be installed on the server which installs the Office Web App service. Office Web App

Product Suites	Product	Detailed Places to Install DocAve Agents
		service includes Word Viewing Service Application, PowerPoint Service Application and Excel Calculation Services. • If you have installed the **Microsoft SQL Server Reporting Services Add-in** for Microsoft SharePoint technologies, and generated stubs for the **Report Builder Model**, you must install DocAve Agent on the server which installs the add-in.
	Connector (In RBS environment)	• DocAve Agents must be installed on all the Web front-end servers. • DocAve Agent must be installed on the server which installs the Office Web App service. Office Web App service includes Word Viewing Service Application, PowerPoint Service Application and Excel Calculation Services. • If you have installed the **Microsoft SQL Server Reporting Services Add-in** for Microsoft SharePoint technologies, and generated stubs for the **Report Builder Model**, you must install DocAve Agent on the server which installs the add-in.
	Connector (In EBS environment)	• DocAve Agents must be installed on the SharePoint Central Administration server and all the Front-end Web servers. • DocAve Agent must be installed on the server which installs the Office Web App service. Office Web App service includes Word Viewing Service Application, PowerPoint Service Application and Excel Calculation Services. • If you have installed the **Microsoft SQL Server Reporting Services Add-in** for Microsoft SharePoint technologies, and generated stubs for the **Report Builder Model**, you must install DocAve Agent on the server which installs the add-in.

Product Suites	Product	Detailed Places to Install DocAve Agents
	Archiver	DocAve Agent must be installed on at least one of the Web front-end servers.
SharePoint Online		DocAve Agent can be installed on any machine with Internet access or on a machine which can access the Internet via proxy

Appendix B: Accessing Hot Key Mode

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

The following is a list 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.

Operation Interface	Hot Key
DocAve Home Page	1
AvePoint Official Website	2
Control Panel	3
Job Monitor	4
Plan Group	5
Health Analyzer	6
Account Information	9
Help and About	0

DocAve Home Page

Operation Interface and Hot Key			
Migration	M	SharePoint Migration	SM
		Lotus Notes Migration	N
		File System Migration	F
		Livelink Migration	L
		eRoom Migration	E
		EMC Documentum Migration	D
		Exchange Public Folder Migration	P
		Quickr Migration	Q
Data Protection	D	Granular Backup & Restore	G
		Platform Backup & Restore DocAve	P
		High Availability	H
		SQL Server Data Manager	S
Administration	A	Administrator	C
		Content Manager	M
		Deployment Manager	D
		Replicator	R
Compliance	C	eDiscovery	E
		Vault	V
Report Center	R	Usage Reports	U
		Infrastructure Reports	I
		Administration Reports	A
		Compliance Reports	C
		DocAve Reports	D

Operation Interface and Hot Key			
		Settings	S
Storage Optimization	S	Real-time Storage Manager	R
		Scheduled Storage Manager	S
		Connector	C
		Archiver	A
Control Panel		P	
Job Monitor		J	
Plan Group		G	
Health Analyzer		H	
Log Out		L	

Appendix C: Migration Source Environment

The following table displays Migration source versions and systems that are supported by DocAve Migrator. DocAve Migrator does not support the versions that are not listed in the table below.

Migration Source	Supported Version	Comment
File System	Windows 2008 R2 Enterprise	
	Windows 2008 R2 SP1 Enterprise	
	Windows 2008 R2 SP1 Standard	
	Windows 2008 SP2 Enterprise 64-bit	
	Windows 2008 SP2 32-bit	
	Windows 7 SP1 64-bit	
	Windows 7 SP1 32-bit	
	Windows Vista SP2 64-bit	
	Windows XP SP3	Partially Supported. Some properties of the file system cannot be retrieved by the API in the **Interop.Shell32.dll** or **WindowsBase.dll** file.
	Windows 2003 R2 SP2 64-bit	
	Windows 2012 RTM	
	Windows 8 32-bit	
	Windows 8 64-bit	
Lotus Notes	English language package 6.5.5	
	English language package 6.5.6	
	English language package 7.0.3	
	English language package 8.0	
	English language package 8.5	
	English language package 8.5.2	
	English language package 8.5.3	
	Japanese language package 6.5.6	
	Japanese language package 8.5	
	German language package 8.5	
	French language package 8.5.3	
	German language package 8.5.2	
	English language package 9.0	
	Japanese language package 9.0	
	German language package 9.0	
eRoom	eRoom 7.2.1	Partially Supported. An error would occur in the source environment while loading the source tree of eRoom 7.2.1, 7.2.2, and 7.2.3 in DocAve
	eRoom 7.2.2	
	eRoom 7.2.3	

Migration Source	Supported Version	Comment
		eRoom Migration. To continue using eRoom Migration, close the error window in the source environment.
	eRoom 7.3	
	eRoom 7.3.3	
	eRoom 7.4.2	
	eRoom 7.4.3	
	eRoom 7.4.4	
Exchange Public Folder	Microsoft Exchange Server 2000	
	Microsoft Exchange Server 2003 32-bit	
	Microsoft Exchange Server 2007 32-bit	Partially Supported. The Web Services access method does not support connecting to this kind of source environment.
	Microsoft Exchange Server 2007 64-bit	
	Microsoft Exchange Server 2007 SP1 32-bit	
	Microsoft Exchange Server 2007 SP1 64-bit	
	Microsoft Exchange Server 2007 SP2 32-bit	
	Microsoft Exchange Server 2007 SP2 64-bit	
	Microsoft Exchange Server 2007 SP3 32-bit	
	Microsoft Exchange Server 2007 SP3 64-bit	
	Microsoft Exchange Server 2010 64-bit	
	Microsoft Exchange Server 2010 SP1 64-bit	
	Microsoft Exchange Server 2010 SP2 64-bit	
	Microsoft Exchange Server 2010 SP3 64-bit	
	Microsoft Exchange Server 2013 64-bit	Partially Supported. AvePoint recommends using the Exchange Public Folder Connection whose access method is MAPI in the same domain with the Exchange Server.
	Microsoft Exchange Server 2013 SP1 64-bit	
Livelink	Livelink 9.5.0	

Migration Source	Supported Version	Comment
	Livelink 9.6.0	
	Livelink 9.7.0	
	Livelink 9.7.1	
	Windows 2003 32-bit	
	Windows 2003 64-bit	
	SQL Server 2000	
	SQL Server 2005 SP2 32-bit	
	SQL Server 2005 SP2 64-bit	
	Oracle 9 32-bit	
	Oracle 10 64-bit	
EMC Documentum	EMC 5.3	
	EMC 6.5	
	EMC 6.6	
Quickr Migration	Quikr 6.5	
	Quikr 7.0.3	
	Quikr 8	

Appendix D: Permission Requirements for DocAve Modules

In order to install and use DocAve modules properly, certain permissions are required. The following sections provide details on the permission requirements for each DocAve module.

Migrator

Refer to the following sections to view the permission requirements for the DocAve Migrator modules. The DocAve Migrator modules include File System Migrator, SharePoint Migrator, Lotus Notes Migrator, EMC Documentum Migrator, eRoom Migrator, Quickr Migrator, Livelink Migrator, and Exchange Public Folder Migrator.

File System Migrator

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

File System Migrator for SharePoint On-Premises

To install and use DocAve File System Migrator for SharePoint on-premises environments properly, ensure that the agent account has the following permissions:

1. Local System Permissions – The permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation.

   ***Note:** Operations of files on the file system require local administration permission. Therefore, make sure that the source Agent account is in the local **Administrators** group.

2. SharePoint Permissions – These permissions must be manually configured prior to using DocAve 6 File System Migrator; they are not automatically configured.

   - User is a member of the **Farm Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
   - Full Control to all zones of all Web applications via User Policy for Web applications.
   - Managed Metadata Service: Term Store Administrator
   - Other permissions required
     - Managed Metadata Service: Full Control
     - Managed Metadata Service: Administrator

3. SQL Permissions – These permissions must be manually configured prior to using DocAve 6 File System Migrator; they are not automatically configured.

    - Member has a Database Role of **db_owner** for all of the databases related to SharePoint, including Content Databases, SharePoint Configuration Database, and Central Admin Database.
    - Member has a Database Role of **db_owner** for Migration Database.
    - Creator and Security Admin permission to SQL Server.

    ***Note**: If a Web application enables the forms based authentication and uses database as the method of forms based authentication, ensure at least one condition:

    - The Agent account has a Database Role of **db_owner** to this database.
    - Specify a user in the **connectionString** node in this Web application's **web.config** profile that has the access to this database. For details, refer to the following steps:

        i. Navigate to **Start** > **Administrative Tools** > **Server Manager** > **Roles** > **Web Server (IIS)** > **Internet Information Services (IIS) Manager**, find the Web application in **Sites** list.

        ii. Right-click the desired Web application and select **Explore**.

        iii. Find the **web.config** file in the pop-up window.

        iv. Open the **web.config** file with Notepad.

        v. Find the **connectionString** node and specify a user that has access to the database that stores FBA security information.

File System Migrator for SharePoint Online

To install and use DocAve File System Migrator for SharePoint Online environments properly, ensure that the following permissions are met:

Local System Permissions for Agent Account

For the registered SharePoint Online site collections, the Agent account is on the Agent machine that will run migration jobs. This machine must have network connection or have configured Agent Proxy Settings. For more information about Agent Proxy Settings, refer to the DocAve 6 Control Panel Reference Guide.

For the registered SharePoint on-premises site collections, the Agent account is on the Agent machine that will run migration jobs. This machine must be the Central Administration server or one of the Web front-end servers of the farm where the registered site collections reside, or the machine that can communicate with the Central Administration server or one of the Web front-end servers.

The Agent account must have proper Local System permissions. These permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations within your organization on

the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.

***Note:** Operations of files on the file system require local administration permission. Therefore, make sure that the source Agent account is in the local **Administrators** group.

Required Permissions for the User Used to Register SharePoint Online Site Collections

The user that is used to register SharePoint Online site collections in **Control Panel** > **Registered SharePoint Sites** > **Manual Input Mode** must have the following permissions to each site collection:

- Full Control permission to the site collection
- Managed Metadata Service – Term Store Administrator
- Other permissions required
    - Managed Metadata Service – Full Control
    - Managed Metadata Service – Administrator

***Note**: If the site collections are registered in **Scan Mode**, make sure the user has the Global Administrator role in Office 365.

Required Permissions for the User Used to Register SharePoint On-Premises Site Collections

The user that is used to register SharePoint on-premises site collections in **Control Panel** > **Registered SharePoint Sites** > **Manual Input Mode** must have the following permissions to each site collection:

- User is a member of the **Site Collection Administrator** group.
    - Managed Metadata Service – Term Store Administrator
- Other permissions required
    - Managed Metadata Service – Full Control
    - Managed Metadata Service – Administrator

***Note**: If the site collections are registered in **Scan Mode**, make sure the user has the Full Control permission to all zones of all Web applications via User Policy for Web Applications.

SharePoint Migrator

To install and use SharePoint Migrator properly, ensure that the Agent accounts in your source and destination SharePoint environments have the required permissions.

***Note**: If a Web application on a destination node enables form-based authentication and uses database as the method of form-based authentication, ensure at least one condition:

- The Agent account has a Database Role of **db_owner** to this database.
- Specify a user in the **connectionString** node in this Web application's **web.config** profile that has the access to this database. For details, refer to the instructions below.

i. Navigate to **Start** > **Administrative Tools** > **Server Manager** > **Roles** > **Web Server (IIS)** > **Internet Information Services (IIS) Manager**, find the desired Web application in the **Sites** list.

ii. Right-click the desired Web application and select **Explore**.

iii. Find the **web.config** file in the pop-up window.

iv. Open the **web.config** file with Notepad.

v. Find the **connectionString** node and specify a user that has access to the database that stores FBA security information.

SharePoint 2007 to 2010 Migration

To install and use SharePoint 2007 to 2010Migration properly, ensure that the Agent account of the SharePoint 2007 and 2010 environments have the following permissions:

1. Local System Permissions – These permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.
2. SharePoint Permissions – These permissions must be manually configured prior to using SharePoint 2007 to 2010 Migration; they are not automatically configured.
    - SharePoint 2007 Permissions:
        - User is a member of the Farm **Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
        - Policy for Web Application: Full Read
        - Personalization Services Permission: All of the granular permissions of the default Shared Service Provider
    - SharePoint 2010 Permissions:
        - User is a member of the Farm **Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
        - Policy for Web Application – Full Control
        - User Profile Service Application Permissions:
            - Use Personal Features
            - Create Personal Site
            - Use Social Features
            - Full Control

        - Managed Metadata Service – Term Store Administrator

3. SQL Permissions – These permissions must be manually configured prior to using SharePoint 2007 to 2010 Migration; they are not automatically configured.

    - SharePoint 2007 Permissions – Database Role of **db_owner** for all the databases related with SharePoint, including Content Databases, Configuration Database, Central Admin Database, and Nintex Workflow Database.
    - SharePoint 2010 Permissions – Database Role of **db_owner** for all the databases related with SharePoint, including Content Databases, Configuration Database, Central Admin Database, and Nintex Workflow Database.

SharePoint 2007 to 2013 Migration

To install and use SharePoint 2007 to 2013 Migration properly, ensure that the Agent account of the SharePoint 2007 and 2013 environments have the following permissions:

1. Local System Permissions – These permissions are automatically configured by DocAve during installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.
2. SharePoint Permissions – These permissions must be manually configured prior to using SharePoint 2007 to 2013 Migration; they are not automatically configured.

    - SharePoint 2007 Permissions:
        - User is a member of the Farm **Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
        - Policy for Web Application – Full Read
        - Personalization Services Permission – All of the granular permissions of the default Shared Service Provider
    - SharePoint 2013 Permissions:
        - User is a member of the Farm **Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
        - Policy for Web Application – Full Control
        - User Profile Service Application permissions:
            - Create Personal Site (required for personal storage, newsfeed, and followed content)
            - Follow People and Edit Profile
            - Use Tags and Notes
            - Full Control
        - Managed Metadata Service – Term Store Administrator

2. SQL Permissions – These permissions must be manually configured prior to using SharePoint 2007 to 2013 Migration; they are not automatically configured.
    - SharePoint 2007 Permissions – Database Role of **db_owner** for all the databases related with SharePoint, including Content Databases, Configuration Database, Central Admin Database, and Nintex Workflow Database.
    - SharePoint 2013 Permissions – Database Role of **db_owner** for all the databases related with SharePoint, including Content Databases, Configuration Database, Central Admin Database, and Nintex Workflow Database.

SharePoint 2010 to 2013 Migration

To install and use SharePoint 2010 to 2013 Migration properly, ensure that the Agent account of the SharePoint 2010 and 2013 environments have the following permissions:

1. Local System Permissions – These permissions are automatically configured by DocAve during installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.
2. SharePoint Permissions – These permissions must be manually configured prior to using SharePoint 2010 to 2013 Migration; they are not automatically configured.
    - SharePoint 2010 Permissions:
        - User is a member of the Farm **Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
        - Policy for Web Application – Full Read
        - User Profile Service Application permissions:
            - Use Personal Features
            - Use Social Features
        - Managed Metadata Service – Term Store Administrator
        - Business Data Connectivity Service– Full Control
        - Search Service – Full Control
    - SharePoint 2013 Permissions:
        - User is a member of the Farm **Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
        - Policy for Web Application – Full Control
        - User Profile Service Application permissions:
            - Create Personal Site (required for personal storage, newsfeed, and followed content)

        - Follow People and Edit Profile
        - Use Tags and Notes
        - Full Control
    - Managed Metadata Service – Term Store Administrator
    - Business Data Connectivity Service – Full Control
    - Search Service – Full Control

3. SQL Permissions – These permissions must be manually configured prior to using SharePoint 2010 to 2013 Migration; they are not automatically configured.
    - SharePoint 2010 Permissions – Database Role of **db_owner** for all the databases related with SharePoint, including Content Databases, Configuration Database, Central Admin Database, and Nintex Workflow Database.
    - SharePoint 2013 Permissions – Database Role of **db_owner** for all the databases related with SharePoint, including Content Databases, Configuration Database, Central Admin Database, and Nintex Workflow Database.

SharePoint Online Permissions

To install and use SharePoint 2007/2010 to SharePoint Online Migration properly, ensure that the Agent account and site collection users (specified when registering site collections) have enough permission.

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

    ***Note**: If the registered site collections are SharePoint Online site collections, the Agent account is on the Agent machine that will run the SharePoint 2007/2010 to SharePoint Online Migration job. This machine must have network connection or have configured Agent Proxy Settings. For detailed information on Agent Proxy Settings, see the **Agent Proxy Settings** section in the DocAve 6 Control Panel Reference Guide.

    If the registered site collections are on-premises site collections, the Agent account is on the Agent machine that will run the SharePoint 2007/2010 to SharePoint Online Migration job. This machine must be the Central Administration server or one of the Web front-end servers of the farm where the registered site collections reside, or the machine that can communicate with the Central Administration server or one of the Web front-end servers.

2. Site Collection User permissions:
    - User is a member of the **Site Collection Administrators** group.

- User Profile Service Application permissions:
    - Follow People and Edit Profile
    - Use Tags and Notes
    - Full Control (only when the registered site collections are on-premises site collections)
- Managed Metadata Service: Term Store Administrator

***Note**: To register site collections using the **Scan Mode**, make sure the specified site collection user has enough permission.

- When the registered site collections are on-premises site collections:

  Policy for Web Application: Full Control

- When the registered site collections are SharePoint Online site collections:

  User has the **Global administrator** role

***Note**: If you want to properly migrate user profile properties to SharePoint Online, the user profile property settings in the source must be configured in prior running the migration job. (In the Office 365 SharePoint admin center, navigate to **user profiles** > **Manage User Properties**. Select the property you want to migrate, and then select **Edit** from the drop-down menu. Select the **Allow users to edit values for this property** option in the **Edit Settings** field, and then click **OK** to save settings.)

Lotus Notes Migrator

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

Lotus Notes Migrator for SharePoint On-Premises

To install and use DocAve Lotus Notes Migrator for SharePoint on-premises properly, ensure that the Agent account has the following permissions:

1. Local System Permissions – The permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.
2. SharePoint Permissions – These permissions must be manually configured prior to using DocAve 6 Lotus Notes Migrator; they are not automatically configured.
    - Member of the **Farm Administrators** group

- Full Control to all zones of all Web applications via User Policy for Web applications
- Managed Metadata Service – Term Store Administrator

- Other permissions required
  - Managed Metadata Service – Full Control
  - Managed Metadata Service – Administrator

3. SQL Permissions – These permissions must be manually configured prior to using DocAve 6 Lotus Notes Migrator; they are not automatically configured.

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

   ***Note**: If forms based authentication (FBA) is selected as a Web application's claims authentication type, ensure at least one of the following conditions is in place:

   - The Agent account must be a member who has a Database Role of **db_owner** for the FBA database.
   - Add the Agent account in the **connectionStrings** node in this Web application's **web.config** file to make the Agent account have the permission to the FBA database. For details, refer to the instructions below.

     i. Navigate to **Start** > **Administrative Tools** > **Server Manager** > **Roles** > **Web Server (IIS)** > **Internet Information Services (IIS) Manager**, find the desired Web application in the **Sites** list.

     ii. Right-click the Web application and select **Explore**.

     iii. A window pops up and you can find the **web.config** file in it.

     iv. Open the **web.config** file with Notepad.

     v. Find the **connectionStrings** node and specify a user that has access to the database that stores FBA security information.

Lotus Notes Migrator for SharePoint Online

To install and use DocAve Lotus Notes Migrator for SharePoint Online environments properly, ensure that the following permissions are met:

Local System Permissions for Agent Account

For the registered SharePoint Online site collections, the Agent account is on the Agent machine that will run migration jobs. This machine must have network connection or have configured Agent Proxy Settings. For more information about Agent Proxy Settings, refer to the DocAve 6 Control Panel Reference Guide.

For the registered SharePoint on-premises site collections, the Agent account is on the Agent machine that will run migration jobs. This machine must be the Central Administration server or one of the Web front-end servers of the farm where the registered site collections reside, or the machine that can communicate with the Central Administration server or one of the Web front-end servers.

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

Required Permissions for the User Used to Register SharePoint Online Site Collections

The user that is used to register SharePoint Online site collections in **Control Panel** > **Registered SharePoint Sites** > **Manual Input Mode** must have the following permissions to each site collection:

- Full Control permission to the site collection
- Managed Metadata Service – Term Store Administrator
- Other permissions required
    - Managed Metadata Service – Full Control
    - Managed Metadata Service – Administrator

***Note**: If the site collections are registered in **Scan Mode**, make sure the user has the Global Administrator role in Office 365.

Required Permissions for the User Used to Register SharePoint On-Premises Site Collections

The user that is used to register SharePoint on-premises site collections in **Control Panel** > **Registered SharePoint Sites** > **Manual Input Mode** must have the following permissions to each site collection:

- User is a member of the **Site Collection Administrator** group.
    - Managed Metadata Service – Term Store Administrator
- Other permissions required
    - Managed Metadata Service – Full Control
    - Managed Metadata Service – Administrator

***Note**: If the site collections are registered in **Scan Mode**, make sure the user has the Full Control permission to all zones of all Web applications via User Policy for Web Applications.

eRoom Migrator

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

eRoom Migrator for SharePoint On-Premises Permissions

To install and use DocAve eRoom Migrator on the SharePoint on-premises environment properly, ensure that the agent account has the following permissions.

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

   ***Note**: Operations of files on the file server that is connected by the UNC path require the **Read** permission at least.

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

   - User is a member of the **Farm Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
   - Full Control to all Web applications via User Policy for Web applications
   - Managed Metadata Service
     - Term Store Administrator
     - Managed Metadata Service Administrator with Full Control Permission

3. SQL Permissions – These permissions must be manually configured prior to using DocAve 6 eRoom Migrator; they are not automatically configured.

   - Member has a Database Role of **db_owner** for all of the databases related to SharePoint, including Content Databases, SharePoint Configuration Database, and Central Admin Database, and DocAve Migration Database.
   - **dbcreator** and **securityadmin** Server Roles in SQL server

   If a Web application enables the forms based authentication and uses database as the method of forms based authentication, ensure at least one of the following conditions is in place:

   - The Agent account has a Database Role of **db_owner** to this database.
   - Specify a user in the **connectionString** node in this Web application's **web.config** profile that has the access to this database. For details, refer to the instructions below:

     i. Navigate to **Start** > **Administrative Tools** > **Server Manager** > **Roles** > **Web Server (IIS)** > **Internet Information Services (IIS) Manager**, find the desired Web application in the **Sites** list.

     ii. Right-click the desired Web application and select **Explore**.

     iii. Find the **web.config** file in the pop-up window.

iv. Open the **web.config** file with **Notepad**.

v. Find the **connectionString** node and specify a user that has access to the database that stores FBA security information.

4. Migration Source Permissions – These permissions must be manually configured prior to using DocAve 6 eRoom Migrator; they are not automatically configured.

    - Full control to eRoom file server

eRoom Migrator for SharePoint Online Permissions

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

1. Agent account permissions:

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

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

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

2. Site Collection user permissions:

    - Member of the **Site Collection Administrators** group of each site collection where you want to use eRoom Migration.
    - Managed Metadata Service
        - Term Store Administrator
        - Managed Metadata Service Administrator with Full Control Permission

***Note**: If using the **Scan Mode** to add the site collections to the SharePoint Sites Group in Control Panel, make sure that the Office 365 account has the **Global Administrator** permission in the specific SharePoint admin center site or the SharePoint account has the Full Control permission for All Zones in the Web application where the site collections reside.

Livelink Migrator

To install and use DocAve Livelink Migrator properly, ensure that the agent account has the following permissions:

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

   ***Note:** The source Livelink Agent account must have the local system permissions. For more information, refer to Local System Permissions. The source Livelink Agent account must have at least **Read** and **Write** permissions to the Livelink objects.

2. SharePoint on-premises Permissions – These permissions must be manually configured prior to using DocAve 6 Livelink Migrator; they are not automatically configured.

   - User is a member of the **Farm Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
   - Full Control to all zones of all Web applications via User Policy for Web applications
   - User Profile Service Application permissions for SharePoint 2010:
     - Use Personal Features
     - Create Personal Site
     - Use Social Features
   - User Profile Service Application permissions for SharePoint 2013:
     - Create Personal Site (required for personal storage, newsfeed, and followed content)
     - Follow People and Edit Profile
     - Use Tags and Notes
   - Managed Metadata Service – Term Store Administrator
   - Other permissions required
     - Managed Metadata Service – Full Control
     - Managed Metadata Service – Administrator
     - User Profile Service – Full Control
     - User Profile Service – Administrator

3. SharePoint Online Permissions: These permissions are required for the user entered when adding site collections to SharePoint Sites Group in Control Panel.

- Full Control to the site collection that you want to use to perform a Livelink Migration job
- Managed Metadata Service – Term Store Administrator
- Other permissions required
    - Managed Metadata Service – Full Control
    - Managed Metadata Service – Administrator

3. SQL Permissions – These permissions must be manually configured prior to using DocAve 6 Livelink Migrator; they are not automatically configured.
    - Member has a Database Role of **db_owner** for all of the databases related to SharePoint, including Content Databases, SharePoint Configuration Database, and Central Admin Database
    - Member has the **dbcreator** and **securityadmin** server roles in SQL Server

If forms based authentication (FBA) is selected as a Web application's claims authentication type, ensure at least one of the following conditions is in place:

- The Agent account must be a member of the **db_owner** database role in the FBA database.
- Add the Agent account in the **connectionStrings** node in this Web application's **web.config** file to make the Agent account have the permission to the FBA database. For details, refer to the instructions below:
    i. Navigate to **Start** > **Administrative Tools** > **Server Manager** > **Roles** > **Web Server (IIS)** > **Internet Information Services (IIS) Manager**, find the desired Web application in the **Sites** list.
    ii. Right-click the desired Web application and select **Explore**.
    iii. Find the **web.config** file in the pop-up window.
    iv. Open the **web.config** file with **Notepad**.
    v. Find the **connectionString** node and specify a user that has access to the database that stores FBA security information.

Exchange Public Folder Migrator

To install and use DocAve Exchange Public Folder Migrator properly, ensure that the Agent account has the following permissions.

Exchange Public Folder to SharePoint On-Premises Migration

To install and use Exchange Public Folder to SharePoint On-Premises Migration properly, ensure that the Agent account have enough permission.

1. Local System Permissions – The permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.
2. SharePoint Permissions – These permissions must be manually configured prior to using Exchange Public Folder to SharePoint On-Premises Migration; they are not automatically configured.
    - User is a member of the **Farm Administrators** group

      ***Note:** Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
    - **Full Control** to all zones of all Web applications via User Policy for Web applications
    - Managed Metadata Service
        - Term Store Administrator
        - Managed Metadata Service Administrator with **Full Control** Permission
3. SQL Permissions – These permissions must be manually configured prior to using Exchange Public Folder to SharePoint On-Premises Migration; they are not automatically configured.
    - Member has a Database Role of **db_owner** in all of the databases related to SharePoint, including Content Databases, SharePoint Configuration Database, and Central Admin Database
    - Member has the Server Roles of **dbcreator** and **securityadmin** in SQL server

    If a Web application enables the forms based authentication and uses database as the method of forms based authentication, ensure at least one of the following conditions is in place:

    - Agent account has a Database Role of **db_owner** to this database.
    - Specify a user in the **connectionString** node in this Web application's **web.config** profile that has the access to this database. For details, refer to the instructions below:

i. Navigate to **Start** > **Administrative Tools** > **Server Manager** > **Roles** > **Web Server (IIS)** > **Internet Information Services (IIS) Manager**, find the desired Web application in the **Sites** list.

ii. Right-click the desired Web application and select **Explore**.

iii. Find the **web.config** file in the pop-up window.

iv. Open the **web.config** file with **Notepad**.

v. Find the **connectionString** node and specify a user that has access to the database that stores FBA security information in the **User ID** and **Password** attributes.

4. Exchange Public Folder Permissions – These permissions must be manually configured prior to using Exchange Public Folder to SharePoint On-Premises Migration; they are not automatically configured.

    - Full Details
    - Folder visible

Exchange Public Folder to SharePoint Online Migration Permissions

To install and use Exchange Public Folder to SharePoint Online Migration properly, ensure that the Agent account and site collection users (specified when registering site collections) have enough permission.

1. Agent account permissions:

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

    ***Note**: If the registered site collections are SharePoint Online site collections, the Agent account is on the Agent machine that will run the Exchange Public Folder to SharePoint Online Migration job. This machine must have network connection or have configured Agent Proxy Settings. For detailed information on Agent Proxy Settings, see the **Agent Proxy Settings** section in the DocAve 6 Control Panel Reference Guide.

    If the registered site collections are on-premises site collections, the Agent account is on the Agent machine that will run the Exchange Public Folder to SharePoint Online Migration job. This machine must be the Central Administration server or one of the Web front-end servers of the farm where the registered site collections reside, or the machine that can communicate with the Central Administration server or one of the Web front-end servers.

2. Site Collection User permissions:
    - User is a member of the **Site Collection Administrators** group.
    - Managed Metadata Service: Term Store Administrator

    ***Note**: To register site collections using the **Scan Mode**, make sure the specified site collection user has enough permission.

    - When the registered site collections are on-premises site collections:

      Policy for Web Application: Full Control

    - When the registered site collections are SharePoint Online site collections:

      User has the **Global administrator** role

3. Exchange Public Folder Permissions: These permissions must be manually configured prior to using Exchange Public Folder to SharePoint Online Migration; they are not automatically configured.
    - Full Details
    - Folder visible

EMC Documentum Migrator

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

EMC Documentum Migrator for SharePoint On-Premises Permissions

To install and use DocAve EMC Documentum Migrator on the SharePoint on-premises environment properly, ensure that the Agent account has the following permissions:

1. Local System Permissions – The permissions are automatically configured by DocAve during the installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.
2. SharePoint Permissions – These permissions must be manually configured prior to using DocAve 6 EMC Documentum Migrator; they are not automatically configured.
    - User is a member of the **Farm Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
    - Full control to all zones of all Web applications via User Policy for Web applications
    - Managed Metadata Service
        - Term Store Administrator

- Managed Metadata Service Administrator with Full Control Permission

3. SQL Permissions – These permissions must be manually configured prior to using DocAve 6 EMC Documentum Migrator; they are not automatically configured.

    - Member has a Database Role of **db_owner** in all of the databases related to SharePoint, including Content Databases, SharePoint Configuration Database, and Central Admin Database.
    - Member has the Server Roles of **dbcreator** and **securityadmin** in SQL server.

    If a Web application enables the forms based authentication and uses database as the method of forms based authentication, ensure at least one of the following conditions is in place:

    - The Agent account has a Database Role of **db_owner** to this database.
    - Specify a user in the **connectionString** node in this Web application's **web.config** profile that has the access to this database. For details, refer to the instructions below:

        i. Navigate to **Start** > **Administrative Tools** > **Server Manager** > **Roles** > **Web Server (IIS)** > **Internet Information Services (IIS) Manager**, find the desired Web application in the **Sites** list.

        ii. Right-click the desired Web application and select **Explore**.

        iii. Find the **web.config** file in the pop-up window.

        iv. Open the **web.config** file with **Notepad**.

        v. Find the **connectionString** node and specify a user that has access to the database that stores FBA security information.

4. Migration Source Permissions – These permissions must be manually configured prior to using DocAve 6 EMC Migrator; they are not automatically configured.

    - Read to EMC Documentum content

    If the DocAve Agent is installed in the machine with the **Documentum DFC Runtime Environment** program installed, ensure the Agent account has the following permissions:

    - Full Control permission to the installation directory of the **Documentum DFC Runtime Environment** program.
    - Add the Agent account to the local **Administrators** group.

EMC Documentum Migration for SharePoint Online Permissions

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

1. Agent account permissions:

    - Local System Permissions: The permissions are automatically configured by DocAve during the installation. Refer to Local System Permissions for a list of the permissions

automatically configured upon installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.

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

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

2. Site Collection user permissions:
    - Member of the **Site Collection Administrators** group of each site collection where you want to use EMC Documentum Migration.
    - Managed Metadata Service
        - Term Store Administrator
        - Managed Metadata Service Administrator with Full Control Permission

***Note**: If using the **Scan Mode** to add the site collections to the SharePoint Sites Group in Control Panel, make sure that the Office 365 account has the **Global Administrator** permission in the specific SharePoint admin center site or the SharePoint account has the Full Control permission for All Zones in the Web application where the site collections reside

Quickr Migrator

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

Quickr Migrator for SharePoint On-Premises

To install and use DocAve Quickr Migrator for SharePoint on-premises environments properly, ensure that the Agent account has the following permissions:

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

    Other permissions – Full Control to Lotus Notes installation path

2. SharePoint Permissions –These permissions must be manually configured prior to using DocAve 6 Quickr Migrator; they are not automatically configured.
    - Member of the Farm Administrators group
        - Full Control to all zones of all Web applications via User Policy for Web applications
        - Managed Metadata Service – Term Store Administrator
    - Other permissions required
        - Managed Metadata Service – Full Control
        - Managed Metadata Service – Administrator
3. SQL Permissions –These permissions must be manually configured prior to using DocAve 6 Quickr Migrator; they are not automatically configured.
    - Member has a Database Role of **db_owner** for all of the databases related to SharePoint, including Content Databases, SharePoint Configuration Database, and Central Admin Database
    - Member has a Database Role of **db_owner** for Migration Database

    ***Note**: If forms based authentication (FBA) is selected as a Web application's claims authentication type, ensure at least one of the following conditions is in place:

    - The Agent account must be a member who has a Database Role of **db_owner** for the FBA database.
    - Add the Agent account in the **connectionStrings** node in this Web application's **web.config** file to make the Agent account have the permission to the FBA database. For details, refer to the instructions below:
        i. Navigate to **Start** > **Administrative Tools** > **Server Manager** > **Roles** > **Web Server (IIS)** > **Internet Information Services (IIS) Manager**, find the desired Web application in the **Sites** list.
        ii. Right-click the Web application and select **Explore**.
        iii. A window pops up and you can find the **web.config** file in it.
        iv. Open the **web.config** file with Notepad.
        v. Find the **connectionStrings** node and specify a user that has access to the database that stores FBA security information.

Quickr Migrator for SharePoint Online

To install and use DocAve Quickr Migrator for SharePoint Online environments properly, ensure that the following permissions are met:

Local System Permissions for Agent Account

For the registered SharePoint Online site collections, the Agent account is on the Agent machine that will run migration jobs. This machine must have network connection or have configured Agent Proxy Settings. For more information about Agent Proxy Settings, refer to the DocAve 6 Control Panel Reference Guide.

For the registered SharePoint on-premises site collections, the Agent account is on the Agent machine that will run migration jobs. This machine must be the Central Administration server or one of the Web front-end servers of the farm where the registered site collections reside, or the machine that can communicate with the Central Administration server or one of the Web front-end servers.

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

***Note**: The source Agent account must have the Full Control permission to Lotus Notes installation path.

Required Permissions for the User Used to Register SharePoint Online Site Collections

The user that is used to register SharePoint Online site collections in **Control Panel** > **Registered SharePoint Sites** > **Manual Input Mode** must have the following permissions to each site collection:

- Full Control permission to the site collection
- Managed Metadata Service – Term Store Administrator
- Other permissions required
    - Managed Metadata Service – Full Control
    - Managed Metadata Service – Administrator

***Note**: If the site collections are registered in **Scan Mode**, make sure the user has the Global Administrator role in Office 365.

Required Permissions for the User Used to Register SharePoint On-Premises Site Collections

The user that is used to register SharePoint on-premises site collections in **Control Panel** > **Registered SharePoint Sites** > **Manual Input Mode** must have the following permissions to each site collection:

- User is a member of the **Site Collection Administrator** group.
    - Managed Metadata Service – Term Store Administrator
- Other permissions required
    - Managed Metadata Service – Full Control
    - Managed Metadata Service – Administrator

***Note**: If the site collections are registered in **Scan Mode**, make sure the user has the Full Control permission to all zones of all Web applications via User Policy for Web Applications.

Local System Permissions

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

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

Data Protection

Refer to the following sections to view the permission requirements for the DocAve Data Protection modules. The DocAve Data Protection modules include Granular Backup and Restore, Platform Backup and Restore, SQL Server Data Manager, and High Availability.

Granular Backup and Restore

Refer to the section below for the required permissions to use Granular Backup and Restore.

Granular Backup and Restore for SharePoint On-Premises Permissions

To install and use Granular Backup and Restore on the SharePoint on-premises environment properly, ensure that the agent account has the required permissions.

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

2. SharePoint Permissions – These permissions must be manually configured prior to using DocAve 6 Granular Backup and Restore; they are not automatically configured.

    - User is a member of the **Farm Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
    - Full Control to all zones of all web applications via User Policy for Web Applications.
    - User Profile Service Application:
        - For SharePoint 2010
            - Use Personal Features
            - Create Personal Site
            - Use Social Features
        - For SharePoint 2013
            - Create Personal Site
            - Follow People and Edit Profile(required for personal storage, newsfeed, and followed content)
            - Use Tags and Notes
    - Managed Metadata Service:
        - Term Store Administrator
        - Administrator with Full Control permission
    - Business Data Connectivity Service: Full Control
    - Search Service: Full Control
    - User Profile Connection Permission:
        - Administrator
        - Full Control

3. SQL Permissions – These permissions must be manually configured prior to using DocAve 6 Granular Backup and Restore; they are not automatically configured.

    - Member has a Database Role of db_owner for all the databases related to SharePoint, including Content Databases, Config Database, and Central Admin Database
        - Creator and Security Admin permission to SQL Server
    - Database Role of **db_owner** for FBA database if forms based authentication (FBA) is enabled in SharePoint Web applications
    - Database Role of **db_owner** for User Profile Service database, Nintex workflow database

Granular Backup and Restore for SharePoint Online Permissions

To install and use Granular Backup and Restore on SharePoint Online environment properly, ensure that the Office 365 account and Agent account have enough permission.

1. Agent account permissions:

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

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

    If the registered site collections are on-premises site collections, the Agent account is on the Agent machine that will run the Granular Backup and Restore job.

2. Site Collection user permissions:

    - User is a member of the **Site Collection Administrators** group.
    - User Profile Service Application permissions:
        - Follow People and Edit Profile
        - Use Tags and Notes
        - Full Control (only when the registered site collections are on-premises site collections)
    - Managed Metadata Service: Term Store Administrator
    - **Read** permission to the **Apps for SharePoint** library in catalog site.

    ***Note**: To register site collections using the **Scan Mode**, make sure the specified site collection user has the following permissions:

    - When the registered site collections are on-premises site collections

      Policy for Web Application: Full Control

    - When the registered site collections are SharePoint Online site collections:

      User has the **Global administrator** role

***Note**: If you want to properly restore user profile properties to SharePoint Online, the user profile property settings in the source must be configured before using Granular Backup and Restore. (In the Office 365 SharePoint admin center, navigate to **user profiles** > **Manage User Properties**. Select the

property you want to restore, and then select **Edit** from the drop-down menu. Select the **Allow users to edit values for this property** option in the **Edit Settings** field, and then click **OK** to save settings.)

Local System Permissions

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

- User is a member of the following local groups:
  - IIS WPG (for IIS 6.0) or IIS IUSRS (for IIS 7.0)
  - Performance Monitor Users
  - DocAve Users (the group is created by DocAve automatically; it has the following permissions):
    - Full Control to the Registry of *HKEY_LOCAL_MACHINE\SOFTWARE\AvePoint\DocAve6*
    - Full Control to the Registry of *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog6*
    - Full Control to the Communication Certificate
    - Permission of Log on as a batch job (navigate to: **Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > User Rights Assignment**)
    - Full Control to the DocAve Agent installation directory

Platform Backup and Restore

To install and use Platform Backup and Restore properly, certain permissions ensure that the Agent account has the following permissions:

Agent Account Configured on SharePoint Servers with Installed Agents included in the Agent Group

1. Local System Permissions – Member of the **Administrator** local group.
2. SharePoint Permissions – This permission must be manually configured prior to using DocAve 6 Platform Backup and Restore; it is not automatically configured.
   - Member of the **Farm Administrators** group

   ***Note:** For SharePoint 2013, the Platform Granular Restore requires the Agent account to have Full Control of all zones of the Web application.

   When restoring the backed up SharePoint 2013 personal site, the Agent account used to run the Platform Granular Restore job must also have the following permissions:

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

- Security account of the application pool used by the Web application where the personal site resides

3. SQL Permissions – These permissions must be manually configured prior to using DocAve 6 Platform Backup and Restore; they are not automatically configured.

    - Database Role of **db_owner** for all the databases related with SharePoint, including SharePoint configuration database, Central Administration content database, all of the content databases, and service application databases
    - Server Role of **public**, **dbcreator** and **securityadmin** in SQL Server
    - Database permission of **View server state** to SQL Server
    - Database permission of **Control server** to SQL Server (this permission is only required when you are using the **AlwaysOn Availability Groups** feature in **SQL Server 2012**, and this permission must be configured on **all SQL instances** inside the **AlwaysOn Availability Group**.)

*Note: The Agent account configured on the Agents that included in the Agent group must have the **View Server State** permission to the SQL Server registered in the staging policy, if the **Enable InstaMount Mapping for Granular Restore** option is selected in the backup plan settings.

Agent Account Configured on Other SharePoint Web Front-end Servers, Except for SQL Server and FAST Search Server

1. Local System Permissions

    - Member of the **Administrators** group

2. SharePoint Permissions

    - Member of the **Farm Administrators** group

3. SQL Permissions

    - Database Role of **db_owner** for the SharePoint configuration database

***Note**: In order to back up the SharePoint Help Search, the user used to start the **SharePoint Foundation Search V4** service must be added to the **Administrators** group on the corresponding machine.

***Note**: In SharePoint 2010, in order to back up the SharePoint Search Service Application, the user (logon user) used to start the **SharePoint Server Search 14** service must be added to the **Administrators** group on the corresponding machine. In SharePoint 2013, the user (logon user) used to start the **SharePoint Search Host Controller** service must be added to the **Administrators** group on the corresponding machine. To configure the equivalent permissions of local Administrator, refer to the following section:

- Full Control to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\VSS\Diag*

- Full Control to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\VSS\VssAccessControl* with **Value data** of **1**
- Member of following local groups: Distributed COM Users, Certificate Service DCOM Access, and WSS_WPG(default)
- Allow launch and activation for the COM security

***Note**: After you have added these permissions to the logon user, restart the services.

Agent Account Configured on the FAST Search Server

1. Local System Permissions
    - Member of the following local groups:
        - **Administrators**
        - **FASTSearchAdministrators** (this permission is only required for the Agent Account configured on the **Fast Search Administration** server)
2. SQL Server
    - Database Role of **public** to SQL Server (this permission is only required for the Agent Account configured on the **Fast Search Administration** server)

Agent Account Configured on the SQL Server

1. Local System Permissions
    - Backup Operator
    - IIS WPG (for IIS 6.0) or IIS IUSRS (for IIS 7.0)
    - Performance Monitor Users
    - DocAve Users
    - DocAve Agent service logon user
    - **Full Control** to the directory of the database files in both of the source and the destination

      ***Note**: The user used to enable the InstaMount must be a member of the local **Administrators** group.
2. SQL Server Permissions
    - Database role of **db-owner** in master database.
    - Database role of **db_owner** in the entire database included in the backup plan.
    - Server role of **dbcreator**, and **processadmin** in SQL server.
    - Database permission of **Control Server** to SQL Server.

***Note**: The user used to back up and restore the certificate encrypted by TDE must have the server role of **securityadmin**.

The user used to restore the SQL logins must have the server role of **securityadmin**.

***Note**: If the user who ran the platform granular restore job is different from the user who run the platform backup job, the user performing the platform granular restore must have the database role of **sysadmin** to SQL Server of the destination.

The user who performed an out of place database level platform restore job must have the database role of **sysadmin** to SQL Server.

The user who ran the platform in place restore with a staging policy using the SQL server of another farm must have the database role of **sysadmin** to SQL server used by the staging policy.

SQL Server Service Account Configured on the SQL Server

The SQL Server Service account configured on the SQL server must have **Read** and **Write** permissions to the **Temporary Buffer**, which is configured in **Control Panel** > **Agent Monitor** > **Configure**.

Local System Permissions

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

User is a member of the following local groups:

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

SQL Server Data Manger

To install and use SQL Server Data Manager properly, ensure that the Agent account has the following permissions:

- Agent Accounts configured on the SharePoint servers where DocAve Agents are installed:
    - SharePoint Permissions – This permission must be manually configured prior to using DocAve 6 SQL Server Data Manager; it is not automatically configured.
        - Member of the **Farm Administrators** group

      ***Note:** For SharePoint 2013, the SQL Server Data Manager requires the Agent account to have Full Control of all zones of the Web application.

      When restoring the backed up SharePoint 2013 personal site, the Agent account used to run the Restore job must also have the following permissions:

        - Full Control to the User Profile Service Application related to the Web application where the personal site resides
        - Security account of the application pool used by the Web application where the personal site resides
    - SQL Permissions – These permissions must be manually configured prior to using DocAve 6 SQL Server Data Manager; they are not automatically configured.
        - Database Role of **db_owner** for all the databases related with SharePoint, including SharePoint Content Database, Configuration Database, Central Administration Database
        - Server Role of **public** for the SQL Server
        - Database Role of **db_owner** for the temporary databases that store the analyzed data
- Users who access the databases of the staging policy:
    - SQL Permissions
        - Server Role of **processadmin** in the SQL Server
        - SQL Instance Permission – Control Server
        - Server Role of **dbcreator** in the SQL Server
        - Server Role of **sysadmin** in the SQL Server
- Agent Accounts configured on the SQL Servers where DocAve Agents are installed:
    - Local System Permissions
        - Member of the **Administrators** group

- SQL Permissions
  - Database Role of **db_owner** for the temporary databases that store the analyzed data
  - Server Role of **public** for the SQL Server

Local System Permissions

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

User must be a member of the following local groups:

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

High Availability

To install and use High Availability properly, refer to the following sections for detailed information.

Required Permissions for SQL Mirroring Method

- Agent account configured on the SharePoint servers that are included in the Agent group.
  - Local System Permissions
    - Member of the **Administrator** local group
  - SharePoint Permissions
    - Member of Farm Administrators group
    - Full Control permission to the User Profile Service Application
  - SQL Permissions – These permissions must be manually configured prior to using DocAve 6 High Availability; they are not automatically configured.

        - Database Role of **db_owner** for SharePoint configuration database, and Central Administration content database
        - Database Role of **db_owner** for all of the databases that you want to perform High Availability jobs on
        - Database Role of **public** to SQL server
        - Database permission of **View server state** to SQL server
        - Database role of **db_owner** for the master database or the **View Any Definition** permission to the SQL server
        - Server role of **dbcreator** or the **Alter Any Database** permission or **View Any Definition** permission to the SQL server
        - Permission of **Control Server** to the destination SQL instance
        - Server role of **securityadmin** to the destination SQL Server

- Agent account configured on the SQL server
    - Local System Permissions
        - Member of the **Administrators** group
    - SQL Server Permissions
        - Database Role of **db_owner** for SQL server master database
        - Database Role of **db_owner** for all of the databases you want to perform the High Availability jobs on
        - Server Role of **dbcreator** and **securityadmin** in SQL server
        - The permissions of **Create Endpoint** and **Alter Login** to SQL server
        - Server Role of **sysadmin** in the destination SQL instance
- SQL Server Service account configured on the SQL server

  The SQL Server Service account configured on the SQL Server must have the following permissions:

    - **Read** and **Write** permissions to the Temporary Buffer, which is configured in **Control Panel** > **Agent Monitor** > **Configure**
    - **Read** and **Write** permissions to the directory of *…\AvePoint\DocAve6\Agent\Jobs*
    - **Read** and **Write** permissions to the sparse file location
- VSS Writer account configured on the SQL Server

  ***Note:** The VSS Writer account configured on the SQL Server must have the **Read** and **Writer** permissions to the database file location (including the path in file share).

- Web application pool account configured on the SQL Server

  If the standby application pool account does not exist in the standby SQL Server and does not have the **db_owner** role to the production database selected for High Availability, the standby application will not be readable, that is, the **Warm Standby** feature is not applicable. To ensure that the Warm Standby feature works, please grant Web application pool account the server role of **sysadmin** in the standby SQL Server

Required Permissions for AlwaysOn Availability Group Method

- Agent account configured on the SharePoint servers that are included in the Agent group.
  - Local System Permissions
    - Member of the **Administrator** local group
  - SharePoint Permissions
    - Member of Farm Administrators group
    - Full Control permission to the User Profile Service Application
  - SQL Permissions – These permissions must be manually configured prior to using DocAve 6 High Availability; they are not automatically configured.
    - Database role of **db_owner** for SharePoint configuration database, and Central Administration content database
    - Database role of **db_owner** for all of the databases that you want to perform High Availability jobs on
    - Database role of **public** to SQL server
    - Database permission of **View server state** to SQL server
    - Permission of **View Any Definition** to SQL server
    - Server role of **dbcreator** or the **Alter Any Database** permission or **View Any Definition** permission to the SQL server
    - Permission of **Control Server** to the destination SQL instance
    - Server role of **securityadmin** to the destination SQL Server
- Agent account configured on the SQL server
  - Local System Permissions
    - Member of the **Administrators** group
  - SQL Server Permissions
    - Database role of **db_owner** for SQL server master database
    - Database role of **db_owner** for all of the databases you want to perform the High Availability jobs on

        - Server role of **dbcreator** and **securityadmin** in SQL server
        - Permission of **View Any Definition** to the SQL server
        - Permission of **Alter Availability Group** to the SQL server
        - Server Role of **sysadmin** in the SQL instance
- SQL Server Service account configured on the SQL server

  The SQL Server Service account configured on the SQL server must have **Read** and **Write** permissions to the **Temporary Buffer** configured in **Control Panel** > **Agent Monitor** > **Configure,** and the **Read** and **Write** permissions to the directory of *…\AvePoint\DocAve6\Agent\Jobs*.

- VSS Writer account configured on the SQL Server

  The VSS Writer account configured on the SQL Server must have the **Read** and **Writer** permissions to the database file location (including the path in file share).

- Web application pool account configured on the SQL Server

  If the standby application pool account does not exist in the standby SQL Server and does not have the **db_owner** role to the production database selected for High Availability, the standby application will not be readable, that is, the **Warm Standby** feature is not applicable. To ensure that the **Warm Standby** feature works, please grant Web application pool account the server role of **sysadmin** in the standby SQL Server.

Required Permissions for Log Shipping Method

- Agent account configured on SharePoint servers that are included in the Agent group.
    - Local System Permissions
        - Member of the **Administrator** group
    - SharePoint Permissions
        - Member of Farm Administrators group
        - Full Control permission to the User Profile Service Application
    - SQL Permissions
        - Database Role of **db_owner** for SharePoint configuration database, and Central Administration content database
        - Database Role of **db_owner** for all of the databases that you want to perform High Availability jobs on
        - Database Role of **public** to SQL server
        - Database permission of **View server state** to SQL server
        - Database Role of **db_owner** for the master database or the **View Any Definition** permission to the SQL server

        - Server role of **dbcreator** or the **Alter Any Database** permission or **View Any Definition** permission to the SQL server
        - Permission of **Control Server** to the destination SQL instance
        - Server role of **securityadmin** to the destination SQL Server
- Agent account configured on the SQL server
    - Local System Permissions
        - Member of the **Administrators** group
    - SQL Server Permissions
        - Database Role of **db_owner** for SQL server master database
        - Database Role of **db_owner** for all of the databases you want to perform the High Availability jobs on
        - Server Role of **dbcreator**, **processadmin**, **securityadmin** in SQL server
        - Permission of **Control Server** to the destination SQL instance
        - Server Role of **sysadmin** in the SQL instance
- SQL Server Service account configured on the SQL server
    - The SQL Server Service account configured on the SQL server must have **Read** and **Write** permissions to the **Temporary Buffer** configured in **Control Panel** > **Agent Monitor** > **Configure**, and the **Read** and **Write** permissions to the directory of *…\AvePoint\DocAve6\Agent\Jobs*
- VSS Writer account configured on the SQL Server

  The VSS Writer account configured on the SQL Server must have the **Read** and **Writer** permissions to the database file location (including the path in file share).
- Web application pool account configured on the SQL Server

  If the standby application pool account does not exist in the standby SQL Server and does not have the **db_owner** role to the production database selected for High Availability, the standby application will not be readable, that is, the **Warm Standby** feature is not applicable. To ensure that the **Warm Standby** feature works, please grant Web application pool account the server role of **sysadmin** in the standby SQL Server.

Administration

Refer to the following sections to view the permission requirements for the DocAve Administration modules. The DocAve Administration modules include Administrator, Content Manager, Deployment Manager, and Replicator.

Administrator

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

Administrator for SharePoint On-Premises Permissions

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

1. Local System Permissions – These permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.
2. SharePoint Permissions – These permissions must be manually configured prior to using DocAve 6 Administrator; they are not automatically configured.
    - User is a member of the **Farm Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
    - Full Control to all zones of all Web applications via User Policy for Web applications.
    - Full Control to the User Profile Service Application related to the Web application where the personal site resides.
3. SQL Permissions – These permissions must be manually configured prior to using DocAve 6 Administrator; they are not automatically configured.
    - Member has a Database Role of **db_owner** for all the databases related to SharePoint, including Content Databases, Config Database, and Central Admin Database.
    - Server Role of **dbcreator** and **securityadmin** in SQL Server.

Administrator for SharePoint Online Permissions

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

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

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

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

2. Site Collection user permissions:
    - Member of the **Site Collection Administrators** group of each site collection where you want to use Administrator Migration.
    - Managed Metadata Service
        - Term Store Administrator

***Note**: If using the **Scan Mode** to add the site collections to the SharePoint Sites Group in Control Panel, make sure that the Office 365 account has the **Global Administrator** permission in the specific SharePoint admin center site or the SharePoint account has the Full Control permission for All Zones in the Web application where the site collections reside.

Local System Permissions

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

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

Content Manager

To install and use Content Manager properly, ensure that the agent account has the following permissions.

1. Local System Permissions – These permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations on the permissions, you can simply add the DocAve Agent Account to the local Administrators group to apply all of the required permissions.
2. SharePoint Permissions – These permissions must be manually configured prior to using DocAve 6 Content Manager; they are not automatically configured.
    - User is a member of the **Farm Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
    - Full Control to all zones of all Web applications via User Policy for Web Applications
    - Full Control to the User Profile Service
    - User Policy for Web Application: Full Control to All zones with Account operates as system option. This permission is needed for restoring the newsfeed.

      ***Note:** To deploy apps, the Agent account cannot be a system account.
    - User Profile Service Application permission:
        - For SharePoint 2010
            - Use Personal Features
            - Create Personal Site
            - Use Social Features
        - For SharePoint 2013
            - Create Personal Site (required for personal storage, newsfeed, and followed content)
            - Follow People and Edit Profile
            - Use Tags and Notes
    - Managed Metadata Service: Term Store Administrator
    - Search Service: Full Control
    - Business Data Connectivity Service: Full Control
3. SQL Permissions – These permissions must be manually configured prior to using DocAve 6 Content Manager; they are not automatically configured.

- **db_owner** database role in all of the databases related with SharePoint, including Content databases, Configuration databases, Central Administration content databases, User Profile Service database, and App Management databases.
- **db_owner** database role in the Nintex Workflow databases, including configuration database and content database.

If a Web application enables the forms based authentication and uses database as the method of forms based authentication, ensure at least one of the following conditions is configured:

- The Agent account has a Database Role of **db_owner** to this database
- Specify a user in the **connectionString** node in this Web application's **web.config** profile that has the access to this database

Local System Permissions

Some local system permissions are automatically configured during DocAve 6 installation. The user will be set up as a member of the following local groups:

- IIS WPG (for IIS 6.0) or IIS IUSRS (for IIS 7.0)
- Performance Monitor Users
- DocAve Users (this group is created by DocAve automatically with the following permissions):
    - Full Control to the Registry of HKEY LOCAL MACHINE\SOFTWARE\AvePoint\DocAve6
    - Full Control to the Registry of HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\eventlog
    - Full Control to the Communication Certificate
    - Permission of Log on as a batch job (navigate to: Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > User Rights Assignment)
    - Full Control Permission for DocAve Agent installation directory

Licensing and Permissions of Content Manager for SharePoint Online

Before using Content Manager for SharePoint Online, ensure that you meet the following prerequisites:

- You have purchased the corresponding license for Content Manager for SharePoint Online.
- You have created SharePoint Sites Group in **Control Panel** and added one or more SharePoint on-premises or SharePoint Online site collections to the SharePoint Sites Group. For more information, refer to the Control Panel Reference Guide.

Required Permissions for Agent Account

To install and use Content Manager properly, ensure that the Agent account has the proper Local System Permissions. DocAve automatically configures the Local System Permissions during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations on the permissions, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.

Required Permissions for the User Used to Register the Site Collection

The permission requirements for the user specified when adding the site collections to SharePoint Sites Group are as follows:

***Note:** The user must have the following permissions to each site collection added to the SharePoint Sites Group.

- 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

Deployment Manager

To install and use Deployment Manager properly, ensure that the agent account has the following permissions:

1. Local System Permissions – These permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations on the permissions, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.
2. SharePoint Permissions – These permissions must be manually configured prior to using DocAve 6 Deployment Manager they are not automatically configured.
    - User is a member of the **Farm Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
    - In SharePoint 2010:
        - Full Control to all zones of all Web applications via User Policy for Web Applications

- In SharePoint 2013:
    - Check the Account operates as System checkbox for Web Applications
- User Profile Service Application permissions:
    - In SharePoint 2010
        - Use Personal Features
        - Create Personal Site
        - Use Social Features
    - In SharePoint 2013
        - Create Personal Site (required for personal storage, newsfeed, and followed content)
        - Follow People and Edit Profile
        - Use Tags and Notes
- Managed Metadata Service: Term Store Administrator
- Search Service: Full Control
- Business Data Connectivity Service: Full Control

3. SQL Permissions – These permissions must be manually configured prior to using DocAve 6Deployment Manager; they are not automatically configured.
    - Database Role of db_owner for all the databases related with SharePoint, including Content Databases, Config Database, and Central Admin Database

Local System Permissions

The following local system permissions are automatically configured during DocAve 6 installation:

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

- Local Administrator

Replicator

To install and use Replicator properly, ensure that the following permissions are met.

Replicator for SharePoint On-Premises

Before using Replicator for SharePoint on-premises, ensure that the Agent account has the following permissions:

1. Local System Permissions – These permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.
2. SharePoint Permissions – These permissions must be manually configured prior to using DocAve 6 Replicator; they are not automatically configured.
    - User is a member of the **Farm Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
    - Full Control to all zones of all Web applications via User Policy for Web Applications
    - For SharePoint 2013, in Policy for Web application, make sure that the DocAve Agent Account has the **Account operates as System** permission if you wish to replicate SharePoint 2013 Social Feed and Follow.
    - User Profile Service Application permissions:
        - For SharePoint 2010
            - Use Personal Features
            - Create Personal Site
            - Use Social Features
        - For SharePoint 2013
            - Create Personal Site
            - Follow People and Edit Profile(required for personal storage, newsfeed, and followed content)
            - Use Tags and Notes
    - Managed Metadata Service: Term Store Administrator
    - Business Data Connectivity Service: Full Control
    - Search Service: Full Control

- User Profile Connection Permission: Full Control

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

    - Database Role of **db_owner** for all the databases related with SharePoint, including Content Databases, Config Database, and Central Admin Database
    - Creator and Security Admin permission to SQL Server
    - Database Role of **db_owner** for FBA database if forms based authentication (FBA) is enabled in SharePoint Web applications.
    - **DB_owner** to Replicator Database

Local System Permissions

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

- User is a member of the following local groups:
    - IIS WPG (for IIS 6.0) or IIS IUSRS (for IIS 7.0)
    - Performance Monitor Users
    - DocAve Users (the group is created by DocAve automatically; it has the following permissions):
        - Full Control to the Registry of *HKEY LOCAL MACHINE\SOFTWARE\AvePoint\DocAve6*
        - Full Control to the Communication Certificate
        - Permission of Log on as a batch job (it can be found within **Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > User Rights Assignment**)
        - Full Control Permission for DocAve Agent installation directory
    - Member of WSS_RESTRICTED_WPG_V4
    - Member of WSS_WPG
    - Member of Administrators (If the SP2010ReplicatorEventhandler.dll does not exist in GAC after the installation, add the agent account to Local Administrator group and then SP2010ReplicatorListener.exe will install the assembly automatically under the agent account.)
    - Full Control to the Registry of "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services"

Replicator for SharePoint Online

Before using Replicator for SharePoint Online, ensure the following permissions are met:

Registered SharePoint On-Premises Site Collections

The following permissions are required for Replicator to manage registered SharePoint on-premises site collections.

Local System Permissions for Agent Account

The Agent account is on the Agent machine that will run replicator jobs. The Agent account must have proper Local System permissions.

DocAve automatically configures the Local System permissions during installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.

- User is a member of the following local groups:
    - IIS WPG (for IIS 6.0) or IIS IUSRS (for IIS 7.0)
    - Performance Monitor Users
    - DocAve Users (the group is created by DocAve automatically; it has the following permissions):
        - Full Control to the Registry of HKEY LOCAL MACHINE\SOFTWARE\AvePoint\DocAve6
        - Full Control to the Communication Certificate
        - Permission of **Log on as a batch job** (it can be found within **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Security Settings** > **Local Policies** > **User Rights Assignment**)
        - Full Control Permission for DocAve Agent installation directory
    - Member of WSS_RESTRICTED_WPG_V4
    - Member of WSS_WPG
    - Member of Administrators (If the SP2010ReplicatorEventhandler.dll does not exist in GAC after the installation, add the agent account to Local Administrator group and then SP2010ReplicatorListener.exe will install the assembly automatically under the agent account.)
    - Full Control to the Registry of "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services"

Required Permissions for the User Used to Register SharePoint On-Premises Site Collections

The user that is used to register SharePoint on-premises site collections in **Control Panel** > **Registered SharePoint Sites** > **Manual Input Mode** must have the following permissions to each site collection:

- User is a member of the **Site Collection Administrator** group.
- User Profile Service Application:
    - Follow People and Edit Profile

    - Use Tags and Notes
    - Full Control
- Managed Metadata Service: Term Store Administrator

***Note**: If the site collections are registered in **Scan Mode**, make sure the user has the Full Control permission to all zones of all Web applications via User Policy for Web Applications.

Registered SharePoint Online Site Collections

The following permissions are required for Replicator to manage registered SharePoint Online site collections.

Local System Permissions for Agent Account

The Agent account is on the Agent machine that has network connection or has configured **Agent Proxy Settings** before registering SharePoint Online site collections. The Agent account must have proper Local System permissions.

DocAve automatically configures the Local System permissions during installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.

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

Required Permissions for the User Used to Register SharePoint Online Site Collections

The user that is used to register SharePoint Online site collections in **Control Panel** > **Registered SharePoint Sites** > **Manual Input Mode** must have the following permissions to each site collection:

- User is a member of the **Site Collection Administrator** group.
- User Profile Service Application:

    - Follow People and Edit Profile
    - Use Tags and Notes
- Managed Metadata Service: Term Store Administrator

***Note**: If the site collections are registered in **Scan Mode**, make sure the user has the Global Administrator role in Office 365.

Compliance

Refer to the following sections to view the permission requirements for the DocAve Compliance modules. The DocAve Compliance modules include eDiscovery, and Vault.

eDiscovery

To install and use eDiscovery properly, the DocAve Agent account must have the following permissions applied:

1. Local System Permissions – These permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.
2. SharePoint Permissions – These permissions must be manually configured prior to using DocAve 6 eDiscovery; they are not automatically configured.
    - Full Control to all zones of all Web applications via User Policy for Web Applications
    - Managed Metadata Service: Term Store Administrator
    - Search Service: Full Control
3. SQL Permissions – These permissions must be manually configured prior to using DocAve 6 eDiscovery; they are not automatically configured.
    - Database Role of db_owner for all the databases related with SharePoint, including content databases, SharePoint configuration database, and Central Admin database.

Local System Permissions

Some local system permissions are automatically configured during DocAve 6 installation. The user will be set up as a member of the following local groups:

- IIS WPG (for IIS 6.0) or IIS IUSRS (for IIS 7.0)
- Performance monitor users
- DocAve users (this group is created by DocAve automatically with following permissions):

- Full Control to the registry of HKEY LOCAL MACHINE\SOFTWARE\AvePoint\DocAve6
- Full Control to the registry of HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\eventlog
- Full Control to the communication certificate
- Permission of Log on as a batch job (it can be found within Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > User Rights Assignment)
- Full Control permission for DocAve Agent installation directory

Vault

To install and use Vault properly, ensure that the Agent Account has the following permissions.

1. Local System Permissions – These permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.
2. SharePoint Permissions – These permissions must be manually configured prior to using DocAve 6 Vault; they are not automatically configured.
   - User is a member of the **Farm Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
   - Full Control to all zones of all Web applications via User Policy for Web Applications
   - User Profile Service Application permissions for SharePoint 2010:
     - Use Personal Features
     - Create Personal Site
     - Use Social Features
   - User Profile Service Application permissions for SharePoint 2013:
     - Create Personal Site (required for personal storage, newsfeed, and followed content)
     - Follow People and Edit Profile
     - Use Tags and Notes
   - Managed Metadata Service – Term Store Administrator
   - Business Data Connectivity Service – Full Control
   - Search Service – Full Control

- User Profile Service – Administrator and Full Control
- Managed Metadata Service – Administrator and Full Control

3. SQL Permissions – These permissions must be manually configured prior to using DocAve 6 Vault; they are not automatically configured.
    - Database Role of **db_owner** for all of the databases related with SharePoint, including Content Databases, SharePoint Configuration Database, and Central Admin Database.

Local System Permissions

Some local system permissions are automatically configured during DocAve 6 installation. The user will be set up as a member of the following local groups:

- IIS WPG (for IIS 6.0) or IIS IUSRS (for IIS 7.0)
- Performance monitor users
- DocAve users (the group is created by DocAve automatically; it has the following permissions):
    - Full Control to the Registry of HKEY_LOCAL_MACHINE\SOFTWARE\AvePoint\DocAve6
    - Full Control to the Registry of HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog6
    - Full Control to the Communication Certificate
    - Permission of Log on as a batch job (it can be found within Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > User Rights Assignment)
    - Full Control Permission for DocAve Agent installation directory

Report Center

In the SharePoint 2010 environment, to install and use Report Center properly, ensure that the Agent account has the following permissions.

1. Local System Permissions – These permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the DocAve Agent Account to the local Administrators group to apply all of the required permissions.
2. SharePoint Permissions – User is a member of the **Farm Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
    - Full Control to all zones of all Web applications via the User Policy for Web Applications

- User Profile Service Application permissions:
    - Full Control
    - Use Personal Features
    - Create Personal Site
    - Use Social Features
- Managed Metadata Service: Term Store Administrator
- Search Service: Full Control

3. SQL Permissions
    - Database Role of **db_owner** for all the databases related with SharePoint, including Content Databases, Config Database, and Central Admin Database
    - **db_owner** of SharePoint 2010 Content Database and Stub Database

      ***Note**: To use the Search Usage report and Referrers report, the users must have the **db_owner** role for SharePoint 2010 Web Analytics Service Databases

      ***Note**: To use the SharePoint Search Service report, the users must have the **db_owner** for the SharePoint 2010 WSS_Logging Database

      ***Note**: To use the Configuration Reports, the users must have the **db_owner** role for the SharePoint 2010 User Profile Service Application Databases

      ***Note**: To use the Best Practice Reports, the users must have the **db_owner** role for the SharePoint 2010 Metadata Service Application Databases

To install and use Report Center properly in the SharePoint 2013 environment, ensure that the Agent account has the following permissions:

1. Local System Permissions – These permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the DocAve Agent Account to the local Administrators group to apply all of the required permissions.
2. SharePoint Permissions – User is a member of the **Farm Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
    - Full Control to all zones of all Web applications via the User Policy for Web Applications
    - User Profile Service Application permissions:
        - Full Control
        - Follow People and Edit Profile

    - Create Personal Site(required for personal storage, newsfeed, and followed content)
    - Use Tags and Notes
- Managed Metadata Service: Term Store Administrator
- Search Service: Full Control

3. SQL Permissions

- Database Role of **db_owner** for all the databases related with SharePoint, including Content Databases, Config Database, and Central Admin Database
- **db_owner** of SharePoint 2013 Content Database and Stub Database

  ***Note**: To use the SharePoint Search Service report, the users must have the **db_owner** role for the SharePoint 2013 WSS_Logging Database

  ***Note**: To use the Configuration Reports, the users must have the **db_owner** role for the SharePoint 2013 User Profile Service Application Databases

  ***Note**: To use the Best Practice Reports, the users must have the **db_owner** role for the SharePoint 2013 Metadata Service Application Databases

Local System Permissions

Some local system permissions are automatically configured during DocAve 6 installation. The user will be set up as a member of the following local groups:

- IIS WPG (for IIS 6.0) or IIS IUSRS (for IIS 7.0, and IIS 8.0)
- Performance Monitor Users
- DocAve Users (the group is created by DocAve automatically; it has the following permissions):
    - Full Control to the Registry of HKEY_LOCAL_MACHINE\SOFTWARE\AvePoint\DocAve6
    - Full Control to the Registry of HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\eventlog
    - Full Control to the Communication Certificate
    - Permission of Log on as a batch job (it can be found within Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > User Rights Assignment)
    - Full Control permission for DocAve Agent installation directory

***Note:** If you want to use **CPU/Memory Usage** or **Networking** reports, you must be the member of local **Administrators** group. If you want to use **Download Ranking**, **Failed Login Attempts**, **IIS Logging**, and

Best Practice Reports or select the **Retrieve IIS Logs** option to retrieve data, you must have Full Control to the path of IIS log files, the path of the **redirection.config** file, and IIS **applicationHost.config** file.

Storage Optimization

Refer to the following sections to view the permission requirements for the DocAve Storage Optimization modules. The DocAve Storage Optimization modules include Storage Manager, Connector, and Archiver.

Storage Manager

The following permissions are required for the Storage Manager agent account; they ensure proper functionality of Storage Manager.

1. Local System Permissions – These permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.
2. SharePoint Permissions
    - User is a member of the **Farm Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
    - Full Control to all zones of all Web applications via User Policy for Web Applications
3. SQL Permissions
    - Database Role of **db_owner** for all the databases related with SharePoint, including content databases, stub databases, SharePoint configuration database and Central Administration content database.
    - Server Role of **dbcreator** in SQL Server since DocAve must create a stub database before performing any Storage Manager job.

Local System Permissions

1. User is a member of the following local groups:
    - **IIS_WPG** (for IIS 6.0) or **IIS_IUSRS** (for IIS 7.0)
    - **Performance Monitor Users**
    - **DocAve Users** (The group is created by DocAve automatically and it has the following permissions)
        - Full Control to the Registry of HKEY_LOCAL_MACHINE\SOFTWARE\AvePoint\DocAve6

- Full Control to the Registry of HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\eventLog6
- Full Control to the Communication Certificate
- Permission of Log on as a batch job (it can be found within Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > User Rights Assignment)
- Full Control Permission of DocAve Agent installation directory

2. Full Control to GAC in order to install Provider dll into GAC.
3. Full Control to **Microsoft SQL Remote Blob Storage** Folder to reconfigure maintainer configuration file.

Connector

Agent Account Permissions

To install and use Connector properly, ensure that the Agent account has the following permissions:

1. Local System Permissions – These permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation.
2. SharePoint Permissions – These permissions must be manually configured prior to using DocAve 6 Connector; they are not automatically configured.
   - User is a member of the **Farm Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
   - Full Control to all zones of all Web applications via User Policy for Web Applications.
3. SQL Permissions – These permissions must be manually configured prior to using DocAve 6 Connector; they are not automatically configured.
   - Member has a Database Role of **db_owner** for all the databases related to SharePoint, including Content Databases, Config Database, and Central Admin Database.
   - Member has a Server Role of **dbcreator** in SQL Server since it must create a stub database before performing any Connector job.

File Share Permissions

Ensure that the user account used by the Connector library to access the file share has the following minimum required permissions:

NTFS Permission	Needed?	Reason Needed
Full Control	No	

NTFS Permission	Needed?	Reason Needed
Traverse folder/Execute File	Yes	Connector traverses the folder in order to access the data within subdirectories. It also needs to be able to open the file directly from the folder.
List Directory/Read Data	Yes	Connector must list all contents within the folder in order to display them within SharePoint. It also needs to read the data in order to provide the binaries via SharePoint.
Read Attributes	Yes	SharePoint has a promotion and demotion feature that reads Office file attributes and then uses them as column data.
Read Extended Attributes	Yes	Office files have extended attributes as well as custom attributes that are used in SharePoint promotion and demotion processes.
Create Files/Write Data	Yes	This permission is needed to create files within the file share when they are created within SharePoint.
Create Directories/Append Data	Yes	This permission is required to create folders within the file share when they are created in SharePoint. Connector creates hidden folders within the file share in order to store version history and prevent other libraries from connecting to the same file share.
Write Attributes	Yes	When SharePoint demotes column information into Office files, the file attributes need to be written to.
Write Extended Attributes	Yes	Office files have extended attributes, as well as custom attributes, that are used in SharePoint promotion and demotion processes.
Delete Subdirectories and Files	Yes	In order to synchronize deletion within SharePoint into the file share, this permission is needed.
Delete	No	Since Connector does not delete the root folder that is connected to, this permission is not needed.
Read Permissions	Yes*	*This permission is needed only when loading NTFS permission information from the file share into an Connector library.
Change Permissions	No	Since Connector does not change permission information within the file share, this permission is not needed.
Take Ownership	No	Since Connector does not attempt to take ownership of a file or folder, this permission is not needed.

Local System Permissions

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

User is a member of the following local groups:

- IIS WPG (for IIS 6.0) or IIS IUSRS (for IIS 7.0)

- Performance Monitor Users
- DocAve Users (the group is created by DocAve automatically; it has the following permissions):
    - Full Control to the Registry of HKEY_LOCAL_MACHINE\SOFTWARE\AvePoint\DocAve6
    - Full Control to the Registry of HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\eventlog
    - Full Control to the Communication Certificate
    - Permission of Log on as a batch job (it can be found within Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > User Rights Assignment)
    - Full Control Permission for DocAve Agent installation directory
- Local Admin (this permission is required to deploy solution files to front-end Web servers)

Archiver

To install and use Archiver properly, ensure that the Agent account has the following permissions.

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

   ***Note:** The Local Administrator permission is required to deploy any Archiver solution.

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

    - User is a member of the **Farm Administrators** group. Since Archiver works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
    - Full Control to all zones of all Web applications via User Policy for Web Applications
    - User Profile Service Application permissions for SharePoint 2010:
        - Member of the Administrators group with Full Control
        - Use Personal Features
        - Create Personal Site
        - Use Social Features
        - Full Control

- User Profile Service Application permissions for SharePoint 2013:
    - Member of the Administrators group with Full Control
    - Create Personal Site (required for personal storage, newsfeed, and followed content)
    - Follow People and Edit Profile
    - Use Tags and Notes
    - Full Control
- Managed Metadata Service:
    - Term Store Administrator
    - Member of the Administrators group with Full Control
    - Full Control
- Business Data Connectivity Service – Full Control
- Search Service – Full Control

3. SQL Permissions – These permissions must be manually configured prior to using DocAve 6 Archiver; they are not automatically configured:
    - Database Role of **db_owner** for all the databases related to SharePoint, including Content Databases, SharePoint Configuration Database, and Central Administration Content Database
    - Database Role of **db_owner** for the Archiver Database, User Profile Database, Nintex Workflow Database, and FBA Authentication Database
    - Server Role of **dbcreator** and **securityadmin** in SQL Server (this permission is only required when you choose to create the **Archiver Database** using the **Windows Authentication** method, because the Agent Account will be used to create the Archiver Database)

      ***Note**: If you choose to use **SQL Authentication** when creating the **Archiver Database**, make sure the user specified also has **dbcreator** and **securityadmin** server roles in SQL Server.

Local System Permissions

Some local system permissions are automatically configured during DocAve 6 installation. The user will be set up as a member of the following local groups:

- IIS WPG (for IIS 6.0) or IIS IUSRS (for IIS 7.0)
- Performance Monitor Users
- DocAve Users (the group is created by DocAve automatically; it has the following permissions):

- Full Control to the Registry of HKEY_LOCAL_MACHINE\SOFTWARE\AvePoint\DocAve6
- Full Control to the Registry of HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\eventLog6
- Full Control to the Communication Certificate
- Permission of Log on as a batch job (it can be found within Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > User Rights Assignment)
- Full Control permission for DocAve Agent installation directory

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 © 2012-2016 AvePoint, Inc. All rights reserved. All materials contained in this publication are protected by United States copyright law and no part of this publication may be reproduced, modified, displayed, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of AvePoint, 3 Second Street, Jersey City, NJ 07311, USA or, in the case of materials in this publication owned by third parties, without such third party's consent.

Trademarks

AvePoint®, DocAve®, the AvePoint logo, and the AvePoint Pyramid logo are registered trademarks of AvePoint, Inc. with the United States Patent and Trademark Office. These registered trademarks, along with all other trademarks of AvePoint used in this publication are the exclusive property of AvePoint and may not be used without prior written consent.

Microsoft, MS-DOS, Internet Explorer, Microsoft Office SharePoint Servers 2007/2010/2013, SharePoint Portal Server 2003, Windows SharePoint Services, Windows SQL server, and Windows are either registered trademarks or trademarks of Microsoft Corporation.

Adobe Acrobat and Acrobat Reader are trademarks of Adobe Systems, Inc.

All other trademarks contained in this publication are the property of their respective owners and may not be used such party's consent.

Changes

The material in this publication is for information purposes only and is subject to change without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, AvePoint makes no representation or warranty, expressed or implied, as to its completeness, accuracy, or suitability, and assumes no liability resulting from errors or omissions in this publication or from the use of the information contained herein. AvePoint reserves the right to make changes in the Graphical User Interface of the AvePoint software without reservation and without notification to its users.

AvePoint, Inc.
Harborside Financial Center, Plaza 10
3 Second Street, 9th Floor
Jersey City, New Jersey 07311
USA