# DocAve® 6 Installation

## User Guide

**Service Pack 7**

**Issued September 2016**

# Table of Contents


What's New in this Guide ..... 7

Submitting Documentation Feedback to AvePoint ..... 8

Introduction ..... 9

Before You Begin ..... 10

AvePoint's Testing Policy and Environment Support ..... 10

Supported Software Environments ..... 10

Supported Hardware ..... 10

Supported Backup and Recovery ..... 10

Notable Environment Exceptions ..... 11

SharePoint Agent Account Permissions ..... 11

Reasons for Agent Account Permissions ..... 12

Local Permissions ..... 12

SQL Permissions ..... 13

SharePoint Permissions ..... 13

Adding DocAve 6 to Your Anti-Virus Exclusion List ..... 14

Ports Used by DocAve 6 ..... 14

Supported Browsers for Accessing DocAve ..... 42

DocAve Manager System Requirements ..... 42

System Requirements for Control Service Installation ..... 43

System Requirements for Media Service Installation ..... 46

System Requirements for Report Service Installation ..... 46

DocAve Agent System Requirements ..... 47

System Requirements for Agent Service Installation ..... 47

SQL Server Requirements for DocAve Databases ..... 48

SharePoint Environment Requirements for DocAve Agents ..... 48

Overview of DocAve Manager Services and DocAve Agent Service ..... 48

Stand-Alone Health Analyzer Tool ..... 49

Using the Health Analyzer Connection Tool ..... 50

Using the Stand-Alone Health Analyzer Tool ..... 50

Configuring the CSV File for Importing the Server Information in Bulk ..... 51
Configuring a Healthy DocAve Environment ..... 52
Compatibility Matrix of DocAve and Governance Automation Versions ..... 52
Installing DocAve 6 ..... 53
DocAve Manager ..... 53
Installing DocAve Manager ..... 53
DocAve Control Service Load Balancing ..... 62
DocAve Agent ..... 65
Installing DocAve Agents ..... 65
Accessing the DocAve GUI ..... 69
Internet Explorer Setup ..... 69
Modifying SSL Certificate of DocAve6 Website ..... 71
Logging into DocAve ..... 72
Out-of-Browser Accessing DocAve Manager ..... 73
After You Install DocAve ..... 75
DocAve Health Analyzer Best Practices ..... 75
DocAve Health Analyzer ..... 75
Managing DocAve Health Analyzer Profiles ..... 77
Creating a DocAve Health Analyzer Profile ..... 78
Configuring Scan Schedule Settings for the DocAve Health Analyzer Profile ..... 79
Managing Rules in a DocAve Health Analyzer Profile ..... 81
Exporting DocAve Health Analyzer Report ..... 81
DocAve Manager and Agent Maintenance ..... 82
Using the DocAve Manager/Agent Configuration Tool ..... 82
Using the DocAve Manager/Agent Restart Service Tool ..... 83
Using the DocAve Manager/Agent Uninstallation Wizard ..... 83
Changing the Manager Installation ..... 84
Repairing the Manager/Agent Installation ..... 84
Uninstalling DocAve ..... 85
Uninstalling DocAve Software ..... 85
Storage Manager ..... 85
Archiver ..... 85

Connector ..... 85
Cloud Connect ..... 86
Uninstalling DocAve Manager ..... 87
Uninstalling DocAve Manager from Common Environments ..... 87
Uninstalling DocAve Manager from Windows Server 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core ..... 88
Uninstalling DocAve Agents ..... 88
Uninstalling DocAve Agent from Common Environments ..... 88
Uninstalling DocAve Agent from Windows Server 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core ..... 90
Advanced Configuration ..... 91
Modifying the Port Used by DocAve Storage Manager, Connector and Cloud Connect ..... 91
Modifying the Port Used by DocAve Replicator ..... 91
Modifying the Port Used by DocAve High Availability ..... 92
Helpful Notes ..... 93
Installed DocAve Agents Cannot be Displayed in the Manager Interface ..... 93
Database Collation Issue ..... 94
Other Issues ..... 95
Appendix A: Where to Install DocAve Agents ..... 96
Appendix B: Accessing Hot Key Mode ..... 105
Using Hot Key Mode in DocAve Home Page ..... 105
Using Hot Key Mode in Health Analyzer ..... 106
Appendix C: Migration Source Environment ..... 108
Appendix D: Permission Requirements for DocAve Modules ..... 111
Migrator ..... 111
File System Migrator ..... 111
SharePoint Migrator ..... 114
Lotus Notes Migrator ..... 123
eRoom Migrator ..... 126
Livelink Migrator ..... 128
Exchange Public Folder Migrator ..... 131
EMC Documentum Migrator ..... 134

Quickr Migrator ..... 137
Local System Permissions ..... 140
Data Protection ..... 141
Granular Backup and Restore ..... 141
Platform Backup and Restore ..... 144
SQL Server Data Manager ..... 149
High Availability ..... 150
VM Backup and Restore ..... 163
Administration ..... 165
Administrator ..... 165
Content Manager ..... 167
Deployment Manager ..... 170
Replicator ..... 173
Compliance ..... 178
eDiscovery ..... 178
Vault ..... 179
Report Center ..... 180
Local System Permissions ..... 182
Storage Optimization ..... 183
Storage Manager ..... 183
Connector ..... 184
Cloud Connect ..... 186
Archiver ..... 187
Appendix E: User-defined Certificates ..... 191
Generating a Certificate ..... 191
Adding the Certificates Snap-in to Microsoft Management Console ..... 191
Creating a Request File ..... 193
Requesting and Downloading a Certificate ..... 196
Importing a Certificate ..... 197
Exporting a Certificate ..... 198
Checking Key Type Using Script ..... 199
Appendix F: Unattended Installation of DocAve Manager ..... 201

Generating the Installation Answer File for DocAve Manager ..... 201
Importing the UnattendedInstallation.dll File ..... 206
Commands and Command Parameters for DocAve Manager Unattended Installation ..... 207
Environment Checking Command ..... 207
Installation Command ..... 209
Getting Configuration Information Command ..... 212
Configuring Configuration Information Command ..... 214
Verifying Configuration Information Command ..... 220
Getting Help Information about DocAve Manager Unattended Installation Commands ..... 225
Appendix G: Unattended Installation of DocAve Agent ..... 226
Generating the Installation Answer File for DocAve Agent ..... 226
Importing the UnattendedInstallation.dll File ..... 227
Commands and Command Parameters for DocAve Agent Unattended Installation ..... 228
Environment Checking Command ..... 229
Installation Command ..... 231
Installing DocAve Agent in Parallel Command ..... 233
Getting Configuration Information Command ..... 234
Configuring Configuration Information Command ..... 236
Verifying Configuration Information Command ..... 239
Getting Help Information About DocAve Agent Unattended Installation Commands ..... 241
Appendix H: Unattended Uninstallation of DocAve Manager ..... 242
Importing the UnattendedInstallation.dll File ..... 242
Command and Command Parameters for DocAve Manager Unattended Uninstallation ..... 243
Appendix I: Unattended Uninstallation of DocAve Agent ..... 245
Importing the UnattendedInstallation.dll File ..... 245
Command and Command Parameters for DocAve Agent Unattended Uninstallation ..... 246
Notices and Copyright Information ..... 248

# What's New in this Guide

- Updated Ports Used by DocAve 6.
- Added SharePoint Server 2016 to SharePoint Environment Requirements for DocAve Agents.
- Updated all migration related products in Appendix A: Where to Install DocAve Agents.
- Updated permission requirements for the following DocAve modules:
    - SharePoint Migrator
    - Platform Backup and Restore
    - SQL Server Data Manager
    - VM Backup and Restore
    - High Availability
    - Content Manager
    - Deployment Manager
    - Replicator
    - Connector
    - Cloud Connect
    - Archiver

# Submitting Documentation Feedback to AvePoint

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

# Introduction

The DocAve Installation Guide is designed to help you through the process of installing and configuring DocAve 6. Below is a brief overview of how to use this guide and how to install DocAve 6.

1. Review and configure the appropriate Local, SQL Server, and SharePoint Permissions and system requirements. See Before You Begin.
2. Install DocAve Manager. See Installing DocAve Manager and Appendix F: Unattended Installation of DocAve Manager.
    - Install DocAve Manager on common environments using DocAve Manager Installation Wizard. See Installing DocAve Manager on Common Environments.
    - Install DocAve Manager on Windows Server Core environments using Command Line. See Installing DocAve Manager on Windows Server 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core.
    - Remotely Install DocAve Manager using DocAve Manager unattended installation commands. See Appendix F: Unattended Installation of DocAve Manager.
3. Install DocAve Agents. See Installing DocAve Agents and Appendix G: Unattended Installation of DocAve Agent.
    - Install DocAve Agent on common environments using DocAve Agent Installation Wizard. See Installing DocAve Agent on Common Environments.
    - Install DocAve Agent on Windows Server Core environments using Command Line. Installing DocAve Agent on Windows Server 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core.
    - Remotely Install DocAve Agent using DocAve Agent unattended installation commands. See Appendix G: Unattended Installation of DocAve Agent.

# Before You Begin

Before you begin installing and configuring DocAve, see the following sections for AvePoint's Testing Policy, Notable Environmental Exceptions, Required Permissions and System Requirements.

## AvePoint's Testing Policy and Environment Support

### Supported Software Environments

AvePoint is committed to testing against all major versions and service packs of SharePoint as well as the latest versions of Windows Server and SQL Server, as Microsoft announces support and compatibility.

***Note:** AvePoint does not recommend or support installing DocAve on client operating systems.

### Supported Hardware

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

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

***Note:** Due to changes in the IBM Tivoli Storage Manager API, DocAve 6 Service Pack 6 and later versions require that TSM Client version 7.1.2 is installed on the Control Service and Media Service servers.

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

### Supported Backup and Recovery

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

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

DocAve supports application and configuration server backups for all the supported software environments listed above. DocAve 6 SP5 supports VM backup via Hyper-V/VMWare for the following operating systems: Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Microsoft Hyper–V Server 2012 R2.

### Notable Environment Exceptions

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

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

## 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:

1. 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. The following are 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.

2. 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.
3. 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 Full control and **account operates as system account** to all zones of all Web applications via User Policy for Web Applications. The system account cannot be used as Agent account for restoring SharePoint apps. To restore SharePoint apps, you must ensure that the Agent account is not a system account.

1. 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.
2. 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

3. Managed Metadata Service
    - Term Store Administrator

      DocAve needs this permission to access and create term or keywords.
4. Business Data Connectivity Service
    - Full Control

      This allows DocAve to get the schema of external content type.
5. 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.<br>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 |

| Port | Usage | Must be Enabled On … |
|---|---|---|
| 14005 | Port used by DocAve Storage Manager, Connector, and Cloud Connect processes to transmit the data required by the enabled EBS/RBS provider. | N/A |
| 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 |
| 14008 | Port used by: DocAve Replicator to transfer data for replication jobs, and back up the source data when the Backup Before Replication option is enabled; by Report Center to transfer data between Report service and Agent service; by eRoom Migration/EMC Documentum Migration/Lotus Notes Migration/Quickr Migration/File System Migration/Exchange Public Folder Migration/Livelink Migration/SharePoint Migration to transfer data between DocAve Agent services; by Content Manager to allow the Agent in the source to communicate with the Agent in the destination; and by Deployment Manager to allow the Agent in the source to communicate with the Agent in the destination. | DocAve Agent Server and Report 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 |
| 14101 | Ports used by Lotus Notes Migration to generate msg files. | N/A |

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

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Control Service Installation | 14000 | ControlTimerService.exe | Communication with other services. | Install Control service. |
| Media Service Installation | 14001 and 14002 | MediaService.exe | Communication with Control service and data transfer. | Install Media service and register it to the Control service. |
| Report Service Installation | 14003 | ReportService.exe | Communication with other services. | Install Report service and register it to the Control service. |
| Agent Service Installation | 14004 | AgentService.exe | Communication with Control service. | Install agent and register it to the Control service. |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Control Panel | 14007 | CommonPatchInstaller.exe<br>PatchControlCli.exe | PatchControlCli.exe process uses this port to communicate with the CommonPatchInstaller.exe processes of other services. | Update all the Manager/Agent services. |
| | A random number between 8000 and 12000. | ManagerToolWebContainer Server.exe | This port is used in the URL of the pop-up interface which appears after starting the ManagerToolWebContainerServer.exe process if Control service is selected when installing/uninstalling an upgrade patch or hotfix. | Pop up an interface to display the installation/uninstallation progress. |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| SharePoint Migration | 14000 (Control service) | ControlTimerService.exe | Communication between Control service, Agent service and Media service. | SharePoint Online Migration; SharePoint Offline Migration. |
| | 14001 and 14002 (Media service) | MediaService.exe | Communication between Control service, Agent service and Media service. Communication between Control service, Agent service and Media service. | SharePoint Offline Migration. |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| | 14004 and 14008 (Agent service) | SP2007To2010Migration.exe | Communication between Control service, Agent service and Media service. | SharePoint Online Migration; SharePoint Offline Migration. |
| | | SP2007To2013Migration.exe | | |
| | | SP2007To2016Migration.exe | | |
| | | SP2010To2013Migration.exe | | |
| | | SP2010To2016Migration.exe | | |
| | | SP2013To2016Migration.exe | | |
| | | SP2007SPMigrationExport.exe | | |
| | | SP2010SPMigrationExport.exe | | |
| | | SP2013SPMigrationExport.exe | | |
| | | SP2007ToSPOnlineMigration.exe | | SharePoint Online Migration. |
| | | SP2010ToSPOnlineMigration.exe | | |
| | | SP2013ToSPOnlineMigration.exe | | |
| | | SP2007ToSPOnlineHSMigration.exe | Communication between Control service and Agent service. | SharePoint High Speed Migration. |
| | | SP2010ToSPOnlineHSMigration.exe | | |
| | | SP2013ToSPOnlineHSMigration.exe | | |
| | | SP2007SPMigrationHSExport.exe | | |
| | | SP2010SPMigrationHSExport.exe | | |
| | | SP2013SPMigrationHSExport.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| File System Migration | 14000 (Control service) | ControlTimerService.exe | Communication between Manager and Agent. | Migrate source data to SharePoint using online migration. |
| | 14004 and 14008 (Agent service) | FileSystemMigrationWorker.exe | Back up the source data. | |
| | | FileSystemMigrationRestore.exe | Restore the source data to the destination. | |
| | | SP2013FileSystemMigrationRestore.exe | | |
| | | SP2013FileSystemMigrationAzureRestore.exe | | |
| | | FileSystemMigrationAzureWorker.exe | | |
| | | SP2016FileSystemMigrationRestore.exe | | |
| | 14004 (Agent service) | FileSystemMigrationExcelBuilder.exe | Generate the metadata Excel file. | |
| | 14002 (Media service) | MediaService.exe | Communication between Control service, Agent service and Media service. | Run a File System Migration job with the High Performance Conversion option enabled. |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| eRoom Migration | 14000 (Control service) | ControlTimerService.exe | Communication between Control service and Agent service. | Migrate source data to SharePoint using online migration; Migrate source data to SharePoint using offline migration. |
| | | SP2016eRoomMigrationRestore.exe | | |
| | 14004 and 14008 (Agent service) | eRoomMigrationRestore.exe | | |
| | | SP2013eRoomMigrationRestore.exe | | |
| | | eRoomMigrationWorker.exe | | |
| | | SP2016eRoomMigrationRestore.exe | | |
| | 14100 | AgentToolEMMultipleProcessesHelper.exe | Communication between AgentToolEMMultipleProcesses Helper.exe and MigratorTool .exe | eRoom Migration Tool |
| | | MigratorTool.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| EMC Documentation Migration | 14000 (Control service) | ControlTimerService.exe | Communication between Manager and Agent. | Migrate source data to SharePoint using online migration. |
| | | SP2016DocumentumMigrationRestore.exe | | |
| | 14004 and 14008 (Agent service) | DocumentumMigrationWorker.exe | | |
| | | DocumentumMigrationRestore.exe | | |
| | | SP2013DocumentumMigrationRestore.exe | | |
| | | SP2016DocumentumMigrationRestore.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Lotus Notes Migration | 14000 (Control service) | ControlTimerService.exe | Communication between Manager and Agent. | Migrate source data to SharePoint using online migration; Migrate source data to SharePoint using offline migration. |
| | 14004 and 14008 (Agent service) | NotesMigrationWorker.exe | Back up the source data. | |
| | | NotesMigrationWorkerSTA.exe | Use a single threshold apartment thread to back up the source data. | |
| | | NotesMigrationRestore.exe | Restore the source data to the destination. | |
| | | SP2013NotesMigrationRestore.exe | | |
| | | SP2016NotesMigrationRestore.exe | | |
| | 14101 | NotesMigrationRestoreMsgClient.exe | The process is only started when Microsoft Outlook (32-bit) is installed in the destination. The process communicates with **NotesMigrationRestore.exe**, **SP2013NotesMigrationRestore.exe**, or **SP2016NotesMigrationRestore.exe** to generate msg files. | **Convert Lotus Notes documents to msg** is enabled in the migration job. |

| Product | Ports used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Livelink Migration | 14000 (Control service) | LivelinkMigrationWorker.exe<br>LivelinkMigrationRestore.exe<br>SP2013LivelinkMigrationRestore.exe<br>LivelinkMigrationAzureWorker.exe<br>SP2013LivelinkAzureMigrationRestore.exe<br>SP2016LivelinkMigrationRestore.exe | Communication between Manager and Agent. | Migrate source data to SharePoint using online migration; Migrate source data to SharePoint using offline migration. |
| | 14004 and 14008 (Agent service) | LivelinkMigrationWorker.exe<br>LivelinkMigrationRestore.exe<br>SP2013LivelinkMigrationRestore.exe<br>LivelinkMigrationAzureWorker.exe<br>SP2013LivelinkAzureMigrationRestore.exe<br>SP2016LivelinkMigrationRestore.exe | Communication between source Agent and destination Agent. | Migrate source data to SharePoint using online migration. |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Exchange Public Folder Migration | 14000 (Control service) | ControlTimerService.exe | Communication between Control service and Agent service. | Exchange Public Folder Online Migration |
| | 14004 and 14008 (Agent service) | PublicFolderMigrationBackup.exe | | |
| | | PublicFolderMigrationRestore.exe | | |
| | | SP2013PublicFolderMigrationRestore.exe | | |
| | | SP2016PublicFolderMigrationRestore.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Quickr Migration | 14000 (Control service) | ControlTimerService.exe | Communication between Manager and Agent. | Migrate source data to SharePoint using online migration. |
| | 14004 and 14008 (Agent service) | QuickrMigrationWorker.exe | Back up the source data. | |
| | | QuickrMigrationRestore.exe | Restore the source data to the destination. | |
| | | SP2013QuickrMigrationRestore.exe | | |
| | | SP2016QuickrMigrationRestore.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Report Center | 14000 (Control service) | ControlTimerService.exe | Communication between Control service, Agent service and Media service. | Collect data, Run report, Show report, Apply Audit rules, Retrieve Audit data |
| | 14001 (Media service) | MediaService.exe | Communication between Control | Disk Space Monitoring |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| | | | service, Agent service and Media service. | |
| | 14004 (Agent service) | SP2010ReportCenter.exe | Communication between Control service, Agent service and Report service. | Collect data, Run report, Show report, Apply Audit rules, Retrieve Audit data, Run Usage Pattern Alerting plans. |
| | | SP2010RCAuditor.exe | | |
| | | SP2010ReportCenterUsagePatternListener.exe | | |
| | | SP2013ReportCenter.exe | | |
| | | SP2013RCAuditor.exe | | |
| | | SP2013ReportCenterUsagePatternListener.exe | | |
| | | SP2016ReportCenter.exe | | |
| | | SP2016RCAuditor.exe | | |
| | | SP2016ReportCenterUsagePatternListener.exe | | |
| | 14003 (Report service) | ReportService.exe | Communication between Control service, Agent service and Report service. | |
| | 14008 | ReportService.exe | Transfer data between Report service and Agent service | Run Report Center jobs. |
| | | SP2010ReportCenter.exe | | |
| | | SP2010RCAuditor.exe | | |
| | | SP2010ReportCenterUsagePatternListener.exe | | |
| | | SP2013ReportCenter.exe | | |
| | | SP2013RCAuditor.exe | | |
| | | SP2013ReportCenterUsagePatternListener.exe | | |
| | | SP2016ReportCenter.exe | | |
| | | SP2016RCAuditor.exe | | |
| | | SP2016ReportCenterUsagePatternListener.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Connector | 14000 (Control service) | ControlTimerService.exe | Communication between Control service and Agent service. | Scheduled Synchronization; Save/Remove Connector setting; Active Connector Feature. |
| | 14004 (Agent service) | AgentService.exe | Communication between Control service and Agent service. | Scheduled Synchronization; Save/Remove Connector setting; Active Connector Feature. |
| | | SP2010ConnectorProcessor.exe | | |
| | | SP2013ConnectorProcessor.exe | | |
| | | SP2016ConnectorProcessor.exe | | |
| | 14005 | SP2010StorageOptimizationSer vice.exe | 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; Access Connector stubs; Save/Delete Connector setting; Upload/Delete/Edit/ Move/Check in/Check out Connector stub; Upload Connector Links. |
| | | SP2013StorageOptimizationSer vice.exe | | |
| | | SP2016StorageOptimizationSer vice.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Cloud Connect | 14000 (Control service) | ControlTimerService.exe | Communication between Control service and Agent service. | Scheduled Synchronization; Save/Remove Cloud Connect setting; |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| | | | | Active Cloud Connect Feature. |
| | 14004 (Agent service) | AgentService.exe | Communication between Control service and Agent service. | Scheduled Synchronization; Save/Remove Cloud Connect setting; Active Cloud Connect Feature. |
| | | SP2010ConnectorProcessor.exe | | |
| | | SP2013ConnectorProcessor.exe | | |
| | | SP2016ConnectorProcessor.exe | | |
| | 14005 | SP2010StorageOptimizationService.exe | It is an internal port of the Cloud Connect process. Cloud Connect works well even if we don't create any Inbound Rule for this port. | Synchronization; Access Cloud Connect stubs; Save/Delete Cloud Connect setting; Upload/Delete/Edit/Move/Check in/Check out Cloud Connect stub; Upload Cloud Connect Links. |
| | | SP2013StorageOptimizationService.exe | | |
| | | SP2016StorageOptimizationService.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Granular Backup and Restore | 14000 (Control service) | ControlTimerService.exe | Communication between Control service, Agent service and Media service. | Granular backup; Granular restore. |
| | 14001 (Media service) | MediaService.exe | Communication between Control service, Agent service and Media service. | Granular backup; Granular restore. |
| | 14004 (Agent service) | SP2010GranularBackup.exe | Communication between Control service, Agent service and Media service. | Granular backup; Granular restore. |
| | | SP2010GranularRestore.exe | | |
| | | SP2013GranularBackup.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| | | SP2013GranularRestore.exe | | |
| | | SP2016GranularBackup.exe | | |
| | | SP2016GranularRestore.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| VM Backup and Restore | 14000 (Control service) | ControlTimerService.exe | Communication between Control service, Agent service and Media service. | VM Backup; VM Restore; VM File restore |
| | 14001 (Media service) | MediaService.exe | Communication between Control service, Agent service and Media service. | VM Backup; VM Restore; VM File restore |
| | 14004 (Agent service) | AgentCommonVMInstaMountFileServer.exe | Communication between Control service, Agent service, Media service, and with each other. | VM Backup; VM Restore; VM File restore |
| | | AgentCommonVMBackupWorker.exe | | |
| | | AgentCommonVMRestoreWorker.exe | | |
| | | AgentCommonVMBrowser.exe | | |
| | | AgentCommonVMFileRestoreWorker.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Platform Backup and Restore | 14000 (Control service) | ControlTimerService.exe | Communication between Control service | Platform Backup; Platform Restore; Farm Rebuild; Farm Clone; Maintenance; Platform Restore at granular level; End-User Restore; Farm Repair; Database Migration and Index Migration. |
| | 14004 (Agent service) | AgentService.exe | Communication between Agent service and each other | Platform Backup; Platform Restore; Farm Rebuild; Farm Clone; Maintenance; Platform Restore at granular level; End-User Restore; Farm Repair; Database Migration and Index Migration. |
| | | AgentCommonPRLiveModeBrowser.exe | | Platform Restore at granular level |
| | | AgentCommonPRMultipleMember.exe | | Platform Backup; Platform Restore; Database Migration and Index Migration |
| | | AgentCommonPRVDIDBBackup.exe | | Platform Backup; |

| | | | | |
|---|---|---|---|---|
| | | AgentCommonPRVDIDBRestore .exe | | Platform Restore |
| | | AgentCommonPRVSSBackup.exe | | |
| | | AgentCommonPRVSSRestore.exe | | |
| | | AgentCommonPRWebDeployment Worker.exe | | |
| | | SP2010PRControlBackup.exe | | |
| | | SP2010PRControlRestore.exe | | |
| | | SP2010PRBrowser.exe | | |
| | | SP2010PRDisasterRecovery Member.exe | | Farm Rebuild; Farm Repair; Farm Clone |
| | | SP2010PRDisasterRecovery Restore.exe | | |
| | | SP2016PlatformItemRestore.exe | | Platform Restore at granular level; End-User Restore |
| | | SP2013PlatformItemRestore.exe | | |
| | | SP2010PlatformItemRestore.exe | | |
| | | SP2010PRIndexBackup.exe | | Platform Backup; Platform Restore. |
| | | SP2010PRIndexRestore.exe | | |
| | | SP2010PRMultipleControl.exe | | |
| | | SP2010PRWFEBackup.exe | | |
| | | SP2010PRWFERestore.exe | | |
| | | SP2016PRWFEBackup.exe | | |
| | | SP2016PRWFERestore.exe | | |
| | | SP2013PRControlBackup.exe | | |
| | | SP2013PRControlRestore.exe | | |
| | | SP2016PRControlBackup.exe | | |

| | | | | |
|---|---|---|---|---|
| | | SP2016PRControlRestore.exe | | |
| | | SP2013PRDisasterRecovery Member.exe | | Farm Rebuild; Farm Repair; Farm Clone |
| | | SP2013PRDisasterRecovery Restore.exe | | |
| | | SP2016PRDisasterRecoveryRestore.exe | | |
| | | SP2016PRDisasterRecoveryMember.exe | | |
| | | SP2013PRIndexBackup.exe | | Platform Backup; Platform Restore. |
| | | SP2013PRIndexRestore.exe | | |
| | | SP2013PRMultipleControl.exe | | |
| | | SP2016PRMultipleControl.exe | | |
| | | SP2013PRWFEBackup.exe | | |
| | | SP2013PRWFERestore.exe | | |
| | | AgentCommonPRBrowser.exe | | |
| | | AgentCommonVDBFileServer.exe | | Platform Backup; Platform Restore at granular level; Maintenance. |
| | 14001 (Media service) | MediaService.exe | Communication with other DocAve services. | Platform Backup; Platform Restore; Platform Restore at granular level. |

| | | | | |
|---|---|---|---|---|
| | 14002 (Media service) | MediaService.exe | Transmit data between DocAve and the storage device. | Platform Backup; Platform Restore; Farm Rebuild; Farm Clone; Maintenance; Platform Restore at granular level; End-User Restore. |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| SQL Server Data Manager | 14000 (Control service) | ControlTimerService.exe | Communication between Control service | SQL Server Data Manager Analyze, Restore |
| | 14004 (Agent service) | AgentCommonSDMRestoreMember.exe | Communication between agent service and each other | SQL Server Data Manager Analyze, Restore |
| | | AgentCommonSDMBrowser.exe | | |
| | | SP2010SDMControlItemRestore.exe | | |
| | | SP2013SDMControlItemRestore.exe | | |
| | | SP2010PlatformItemRestore.exe | | |
| | | SP2013PlatformItemRestore.exe | | |
| | | SP2016SDMControlItemRestore.exe | | |
| | | SP2016PlatformItemRestore.exe | | |
| | | SP2016AgentCommonBrowser.exe | | |
| | | AgentCommonPRLiveModeBrowser.exe | | |
| | | AgentCommonInstaMountFileServer.exe | | |
| | | AgentCommonBrowser.exe | | |
| | | SP2013AgentCommonBrowser.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| High Availability | 14000 (Control service) | ControlTimerService.exe | Communication between Control service | High Availability Pre-Scan, Synchronizati |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| | | | | on, Failover, Fallback |
| | 14004 (Agent service) | AgentCommonHADataTransferServices.exe | Communication between Agent service and each other | High Availability Pre-Scan, Synchronization, Failover, Fallback |
| | | AgentCommonHASyncWorker.exe | | |
| | | SP2010HABrowser.exe | | |
| | | SP2010HASyncController.exe | | |
| | | SP2010HAFailoverController.exe | | |
| | | SP2010HAMultipleMember.exe | | |
| | | AgentCommonHABrowser.exe | | |
| | | SP2013HASyncController.exe | | |
| | | SP2013HAFailoverController.exe | | |
| | | SP2013HAMultipleMember.exe | | |
| | | SP2016HASyncController.exe | | |
| | | SP2016HAFailoverController.exe | | |
| | | SP2016HAMultipleMember.exe | | |
| | 14007 (Agent service) | AgentCommonHADataTransferServices.exe | Transfer data between production SQL Agent and standby SQL Agent<br>***Note**: For details on changing the data transfer port, refer to Modifying the Port Used by DocAve High Availability | High Availability Synchronization |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Deployment Manager | 14000 (Control service) | ControlTimerService.exe | Communication between Control service and Agent service. | Online Deployment Manager jobs; Offline Deployment Manager jobs. |
| | | ReportService.exe | | |
| | | AgentService.exe | | |
| | | MediaService.exe | | |
| | 14001 (Control service) | ControlTimerService.exe | Communication between Control service, Agent service and Media service. | Deployment Manager jobs that checked the Backup the destination environment checkbox; Solution Store. |
| | 14002 (Media service) | SP2013GranularBackup.exe | Transfer data between Media service and Agent service. | Deployment Manager jobs that checked the Backup the destination environment checkbox; Solution Store. |
| | | SP2013GranularRestore.exe | | |
| | | SP2010GranularBackup.exe | | |
| | | SP2010GranularRestore.exe | | |
| | | SP2016GranularRestore.exe | | |
| | | SP2016GranularBackup.exe | | |
| | 14008 | SP2013DMAppHostPrimary.exe | Transfer data in Deployment Manager jobs. | Online Deployment Manager jobs; Offline Deployment Manager jobs. |
| | | SP2013DMAppHostSecondary.exe | | |
| | | AgentCommon2013ComparePrimary .exe | | |
| | | AgentCommon2013Compare Secondary.exe | | |
| | | SP2013SCDMAppHostPrimary.exe | | |
| | | SP2013SCDMAppHostSecondary.exe | | |
| | | SP2013WFEDMAppHostPrimary.exe | | |
| | | SP2013WFEDMAppHostSecondary.exe | | |
| | | SP2013MMSAppHostPrimary.exe | | |
| | | SP2013MMSAppHostSecondary.exe | | |
| | | SP2010DMAppHostPrimary.exe | | |
| | | SP2010DMAppHostSecondary.exe | | |
| | | AgentCommon2010ComparePrimary .exe | | |
| | | AgentCommon2010Compare Secondary.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| | | SP2010MMSAppHostPrimary.exe | | |
| | | SP2010MMSAppHostSecondary.exe | | |
| | | SP2010WFEDMAppHostPrimary.exe | | |
| | | SP2010WFEDMAppHostSecondary.exe | | |
| | | SP2010SCDMAppHostPrimary.exe | | |
| | | SP2010SCDMAppHostSecondary.exe | | |
| | | SP2016DMAppHostPrimary.exe | | |
| | | SP2016DMAppHostSecondary.exe | | |
| | | AgentCommon2016ComparePrimary.exe | | |
| | | AgentCommon2016CompareSecondary.exe | | |
| | | SP2016SCDMAppHostPrimary.exe | | |
| | | SP2016SCDMAppHostSecondary.exe | | |
| | | SP2016WFEDMAppHostPrimary.exe | | |
| | | SP2016WFEDMAppHostSecondary.exe | | |
| | | SP2016MMSAppHostPrimary.exe | | |
| | | SP2016MMSAppHostSecondary.exe | | |
| | 14004 (Agent service) | SP2013DMAppHostPrimary.exe | Communication between Control service and Agent service. | Online Deployment Manager jobs; Offline Deployment Manager jobs. |
| | | SP2013DMAppHostSecondary.exe | | |
| | | ControlTimerService.exe | | |
| | | SP2013AgentCommonBrowser.exe | | |
| | | AgentCommon2013ComparePrimary.exe | | |
| | | AgentCommon2013CompareSecondary.exe | | |
| | | SP2013SCDMAppHostPrimary.exe | | |
| | | SP2013SCDMAppHostSecondary.exe | | |
| | | SP2013WFEDMAppHostPrimary.exe | | |
| | | SP2013WFEDMAppHostSecondary.exe | | |
| | | SP2013MMSAppHostPrimary.exe | | |
| | | SP2013MMSAppHostSecondary.exe | | |
| | | SP2010DMAppHostPrimary.exe | | |
| | | SP2010DMAppHostSecondary.exe | | |
| | | AgentCommon2010ComparePrimary.exe | | |
| | | AgentCommon2010CompareSecondary.exe | | |
| | | SP2010MMSAppHostPrimary.exe | | |
| | | SP2010MMSAppHostSecondary.exe | | |
| | | SP2010WFEDMAppHostPrimary.exe | | |
| | | SP2010WFEDMAppHostSecondary.exe | | |
| | | SP2010SCDMAppHostPrimary.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| | | SP2010SCDMAppHostSecondary.exe | | |
| | | SP2010AgentCommonBrowser.exe | | |
| | | SP2016DMAppHostPrimary.exe | | |
| | | SP2016DMAppHostSecondary.exe | | |
| | | SP2016AgentCommonBrowser.exe | | |
| | | AgentCommon2016ComparePrimary.exe | | |
| | | AgentCommon2016CompareSecondary.exe | | |
| | | SP2016SCDMAppHostPrimary.exe | | |
| | | SP2016SCDMAppHostSecondary.exe | | |
| | | SP2016WFEDMAppHostPrimary.exe | | |
| | | SP2016WFEDMAppHostSecondary.exe | | |
| | | SP2016MMSAppHostPrimary.exe | | |
| | | SP2016MMSAppHostSecondary.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Content Manager | 14000 (Control service) | ControlTimerService.exe | Communication with the Control service. | Create a Content Manager plan and run it. |
| | 14001 and 14002 (Media service) | MediaService.exe | Communication 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 (Agent service) | AgentService.exe | Communication with the Agent service. | Run a Content Manager job. |
| | 14008 (Agent service) | SP2010CMAppHostPrimary.exe | Communication between the Agent service in the source with the Agent service in the destination. | Run an Online Content Manager Job. |
| | | SP2010CMAppHostSecondary.exe | | |
| | | SP2013CMAppHostPrimary.exe | | |
| | | SP2013CMAppHostSecondary.exe | | |
| | | SP2016CMAppHostPrimary.exe | | |
| | | SP2016CMAppHostSecondary.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Replicator | 14000 (Control service) | ControlTimerService.exe | Communication between Control service and Agent service. | Online Replicator job; Offline Replicator job; One-way Pull; Real-Time Replicator job; Publishing mode replication job. |
| | 14004 (Agent service) | SP2010ReplicatorOffline.exe | | |
| | | SP2010ReplicatorPrimary.exe | | |
| | | SP2010ReplicatorSecondary.exe | | |
| | | SP2010GranularBackup.exe | | |
| | | AgentCommonReplicatorOffline.exe | | |
| | | AgentCommonReplicatorPrimary.exe | | |
| | | AgentCommonReplicatorSecondary.exe | | |
| | | AgentCommonReplicatorService.exe | | |
| | | AgentCommonGranularBackup.exe | | |
| | 14002 (Media service) | MediaService.exe | Communication between Control service, Agent service and Media service. | Run a Replicator job with the Backup Before Replication option enabled. |
| | 14006 (Agent service) | AgentCommonReplicatorService.exe | Replicator event handler uses this port to send event message to the AgentCommonReplicatorService process. | Real-Time Replicator job; Publishing mode replication job. |
| | 14008 (Agent service) | SP2010ReplicatorPrimary.exe | Transfer data for replication jobs. | Online replication job; Offline replication job; One-way pull replication job. |
| | | SP2010ReplicatorSecondary.exe | | |
| | | AgentCommonReplicatorPrimary.exe | | |
| | | AgentCommonReplicatorSecondary.exe | | |
| | | AgentCommonReplicatorWorker.exe | Use this port to transfer the data | |

| | | | | |
|---|---|---|---|---|
| | 14009 (Agent service) | AgentCommonReplicatorWorker.exe | generated by publishing mode replication and Real-Time replication. | Publishing mode Replicator job; Real-Time Replicator job. |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| eDiscovery | 14000 (Control service) | ControlTimerService.exe | Communication between Control service and Agent service. | Search; Apply Hold; Apply Search Plan. |
| | 14004 (Agent service) | SP2010eDiscoveryExport.exe | Run Search, Export, and Hold jobs. | Search; Export; Hold. |
| | | SP2010eDiscoveryHold.exe | | |
| | | SP2010eDiscoverySearch.exe | | |
| | | SP2013eDiscoveryExport.exe | | |
| | | SP2013eDiscoveryHold.exe | | |
| | | SP2013eDiscoverySearch.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Vault | 14000 (Control service) | ControlTimerService.exe | Communication between Control service and Agent service. | Vault Export job. |
| | 14004 (Agent service) | SP2013ComplianceVaultWorker.exe | Communication between Control service and Agent service. | Vault Export job. |
| | | SP2010ComplianceVaultWorker.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Archiver | 14000 (Control service) | ControlTimerService.exe | Communication between Control service, | Archiver; End-User Archiver; Archiver Restore; Retention. |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| | | | Agent service and Media service. | |
| | 14001 and 14002 (Media service) | MediaService.exe | Communication between Control service, Agent service and Media service. | Archiver; End-User Archiver; Archiver Restore. |
| | 14004 (Agent service) | SP2013StorageProcessingPool.exe | Communication between Control service, Agent service and Media service. | Archiver; End-User Archiver; Archiver Restore; Retention. |
| | | SP2013StorageProcessor.exe | | |
| | | SP2013GranularRestore.exe | | |
| | | SP2016StorageProcessingPool.exe | | |
| | | SP2016StorageProcessor.exe | | |
| | | SP2016GranularRestore.exe | | |
| | | AgentCommonStorageProcessingPool.exe | | |
| | | SP2010StorageProcessor.exe | | |
| | | SP2010GranularRestore.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Storage Manager | 14000 (Control service) | ControlTimerService.exe | Communication 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 (Agent service) | AgentCommonStorageProcessingPool.exe | Communication 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. |
| | | SP2010StorageProcessor.exe | | |
| | | SP2010StorageRestore.exe | | |
| | | SP2013StorageProcessingPool.exe | | |
| | | SP2013StorageProcessor.exe | | |
| | | SP2013StorageRestore.exe | | |
| | | SP2016StorageProcessingPool.exe | | |
| | | SP2016StorageProcessor.exe | | |
| | | SP2016StorageRestore.exe | | |
| | 14005 | SP2010StorageOptimizationService.exe | Transmit the data required by the enabled EBS/RBS provider. | Real-time Storage Manager; Access Storage Manager stubs; Clean up orphan BLOBs. |
| | | SP2013StorageOptimizationService.exe | | |
| | | SP2016StorageOptimizationService.exe | | |

| Product | Ports Used | Related Processes | Usage | Basic Functions Involved |
|---|---|---|---|---|
| Administrator | 14000 (Control service) | ControlTimerService.exe | Communication between Control service and Agent service. | All Administrator functions, including functions on the **Configuration**, **Security**, **Management**, and **Policy Enforcer** tabs. |
| | 14004 (Agent service) | AgentCommonBrowser.exe | Communication between Control service and Agent service. | |
| | | SP2013AgentCommonBrowser.exe | | |
| | | SP2010CentralAdminWorker.exe | | |
| | | SP2013CentralAdminWorker.exe | | |
| | | SP2016AgentCommonBrowser.exe | | |
| | | SP2016CentralAdminWorker.exe | | |

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 text box.
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**.

## Supported Browsers for Accessing DocAve

The following table provides the browser and Silverlight versions supported for accessing the DocAve GUI.

| Rules | Requirements |
|---|---|
| Silverlight Version | 5.0 or later |
| Internet Explorer | 10, 11 |
| Google Chrome* | Earlier than 45.0 |
| Mozilla Firefox | 43.0 |

*As of April 2015, NPAPI plugins are disabled in Chrome. It is not possible to install Silverlight and access DocAve using Chrome unless you perform the workaround detailed in the following Chrome developer blog. Note that this workaround is temporary and will not work beyond September 2015.

## DocAve Manager System Requirements

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

- **Control service** – Manages all DocAve operations and allows users to interact with the web-based DocAve platform. All agents 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 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 G | 60 G for system drive |
| Single Server with Control service, Media service, Report service using Built-in Database | 64-bit, 4 cores | 6 G | 80 G for system drive |

***Note**: AvePoint recommends you not use a Built-in Database to install Manager services, this is because the SQL Server Express has a limitation in the size of the databases.

## System Requirements for Control Service Installation

### Windows Server 2008 and 2012 Requirements

| Elements | Requirements |
|---|---|
| Operating System | Windows Server 2008, Windows Server 2008 R2, Windows Server 2008 R2 SP1 Server Core, Windows Server 2012, Windows Server 2012 R2, Windows Server 2012 Server Core, Windows Server 2012 R2 Server Core |
| Number of CPU Cores | Recommended: 2 or greater |
| Available Physical Memory | Required: 256 MB<br>Recommended: 2 GB or greater |
| Available Disk Space | Required: 1 GB |
| .Net Framework Version | .NET Framework 3.5.1 is required to run the installer.<br>.NET Framework 4.0, 4.5, 4.5.2, 4.6, and 4.6.1 are also supported. |
| .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.<br><br>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<br>• Process Model, .NET Environment and Configuration APIs are installed |

| Elements | Requirements |
|---|---|
| World Wide Web Publishing Service | World Wide Web Publishing Service is started |
| Web Server(IIS) Role | Windows features installed:<br>• Web Server<br>• Common HTTP Features (Static Content, Default Document)<br>• For Windows Server 2008 SP2 and Windows Server 2008 R2 SP1: Application Development (ASP.NET, .NET Extensibility, ISAPI Extensions and ISAPI Filters)<br>• For Windows Server 2012 and Windows Server 2012 R2: Application Development (ASP.NET 3.5, .NET Extensibility 3.5, ISAPI Extensions and ISAPI Filters)<br>• Management Tools (IIS Management Console, IIS 6 Management Compatibility and IIS 6 Metabase Compatibility)<br>***Note**: IIS Management Console is not required to Windows Server Core environment. |
| IIS Admin Service | IIS Admin Service is started<br>IIS version must be 6 or above |
| PowerShell Version | PowerShell 2.0 or above |

## Windows Server 2003 Requirements

| Elements | Requirements |
|---|---|
| Operating System | Windows Server 2003, Windows Server 2003 R2 |
| Number of CPU Cores | Recommended: 2 or greater |
| Available Physical Memory | Required: 256 MB<br>Recommended: 2 GB or greater |
| Available Disk Space | Required: 1 GB |
| .Net Framework Version | .NET Framework 3.5.1 is required to run the installer.<br>.NET Framework 4.0 is also supported. |
| 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.<br>• Internet Information Services (IIS) is started, including the following installed features:<br>  ○ Common Files<br>  ○ IIS Manager<br>  ○ World Wide Web Service |

| Elements | Requirements |
|---|---|
| IIS Service | IIS Admin Service is started<br>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 or IIS8 | 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 or creating an 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

| Element | Requirements |
|---|---|
| Operating System | Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2008 R2 SP1 Server Core, Windows Server 2012, Windows Server 2012 R2, Windows Server 2012 Server Core, Windows Server 2012 R2 Server Core |
| Number of CPU Cores | Recommended: 2 or greater |
| Available Physical Memory | Required: 128 MB<br>Recommended: 1 GB or greater |
| Available Disk Space | Required: 1 GB |
| .NET Framework Version | .NET Framework 3.5.1 is required to run the installer.<br>.NET Framework 4.0, 4.5, 4.5.2, 4.6, and 4.6.1 are also supported. |
| .Net Framework 3.5 Features (only in Windows Server 2008, Windows Server 2008 R2, 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.<br><br>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

| Element | Requirements |
|---|---|
| Operating System | Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2008 R2 SP1 Server Core, Windows Server 2012, Windows Server 2012 R2, Windows Server 2012 Server Core, Windows Server 2012 R2 Server Core |
| Number of CPU Cores | Recommended: 2 or greater |
| Available Physical Memory | Required: 128 MB<br>Recommended: 1 GB or greater |
| Available Disk Space | Required: 1 GB |
| .NET Framework Version | .NET Framework 3.5.1 is required to run the installer.<br>.NET Framework 4.0, 4.5, 4.5.2, and 4.6 are also supported. |

| Element | Requirements |
|---|---|
| .Net Framework 3.5 Features (only in Windows Server 2008, Windows Server 2008 R2, 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.<br><br>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: the 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 choose different accounts for different farms when 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

| Element | Requirements |
|---|---|
| Operating System | Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2008 R2 SP1 Server Core, Windows Server 2012, Windows Server 2012 R2, Windows Server 2012 Server Core, Windows Server 2012 R2 Server Core |
| Number of CPU Cores | Recommended: 2 or greater |
| Available Physical Memory | Required: 256 MB<br>Recommended: 2 GB or greater |
| Available Disk Space | Required: 1 GB |
| .NET Framework Version | .NET Framework 3.5.1 is required to run the installer.<br>.NET Framework 4.0, 4.5, 4.5.2, 4.6, and 4.6.1 are also supported.<br><br>***Note**: To register a SharePoint Online site collection to a SharePoint Sites Group, at least one Agent server in the Agent Group must have .NET 4.5 Framework or later installed. For more information about adding SharePoint Online site collections, see the Control Panel Reference Guide. |
| .Net Framework 3.5 Features (only in Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, | For Windows Server 2008 SP2 and Windows Server 2008 R2 SP1: Windows .NET Framework 3.5.1 must be installed. |

| Element | Requirements |
|---|---|
| and Windows Server 2012 R2 environments) | 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 SP7:<br>• Microsoft SQL Server 2005<br>• Microsoft SQL Server 2008<br>• Microsoft SQL Server 2008 R2<br>• Microsoft SQL Server 2012<br>• Microsoft SQL Azure<br>• Microsoft SQL Server 2012 Business Intelligence<br>• Microsoft SQL Server 2014<br>• SQL Server 2014 Business Intelligence<br>*__Note:__ Not all DocAve 6 features are supported on SharePoint instances that use SQL Server Express. |
| Report Database | |
| Auditor Database | |
| Replicator Database | |
| Stub Database | |
| Policy Enforcer Database | |
| Migrator Database | |
| Archiver Database | |
| Item Caching 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*)
- Microsoft SharePoint Server 2016 RTM

***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 services 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 that only 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
- VM Backup and Restore
- Archiver
- Deployment Manager
- Replicator
- Content Manager
- eDiscovery
- SharePoint  Migration (Offline Migration)
- File System Migration
- Report Center (DocAve Reports)

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.

## Stand-Alone Health Analyzer Tool

The Stand-Alone Health Analyzer Tool is a light-weight software package designed to help users diagnose and solve potential installation problems—specifically related to prerequisite connection, permission, and port configurations—before a DocAve installation. Prior to an installation, the Health Analyzer Tool, in conjunction with the Health Analyzer Connection Tool, can be used to check the connections from the Manager or Agent service server where it is hosted to the server where you are about to install an Agent service, Control service, Media service, and/or Report service .

The Stand-Alone Health Analyzer Tool can also be used before an installation to check the requirements of the Agent account for selected modules and the permissions of the application pool account.  To use the Stand-Alone Health Analyzer Tool, follow the steps below:

1. Activate the Health Analyzer Connection Tool on the servers that will be targeted by the Health Analyzer Tool. See Using the Health Analyzer Connection Tool for more information.

2. Run the Health Analyzer Tool from the Manager or Agent service server. See Using the Stand-Alone Health Analyzer Tool for more information.

Download a copy of the Stand-Alone Health Analyzer Tool here.

## Using the Health Analyzer Connection Tool

The Health Analyzer Connection Tool is used to emulate the port of the server where you are about to install an Agent service, Control service, Media service, and/or Report service, in order to help the Health Analyzer Tool check server connections.

Once the tool package has been loaded onto the server where you are about to install an Agent service, Control service, Media service, and/or Report service, follow the directions below to run the tool:

1. Unzip the tool package and double-click the Health Analyzer Connection Tool in folder Health Analyzer.
2. Enter the port number of the server where you are about to install an Agent service, Control service, Media service, and/or Report service. For more information on the port numbers used, see Ports Used by DocAve 6.
3. Click **Start**.
4. Once the port has been emulated, go to Using the Stand-Alone Health Analyzer Tool and follow the instructions there to check the server connections.

## Using the Stand-Alone Health Analyzer Tool

The Stand-Alone Health Analyzer Tool is used to check if the Agent and/or Manager requirements are met on the server. Additionally, the Health Analyzer Tool can be used to check the hosting server's connection to other servers where you are about to install or have installed an Agent service, Control service, Media service and/or Report service.

The Health Analyzer Tool runs scans on the indicated servers using the inputted criteria and selected rules, looking for errors. After the scan is complete, a report appears detailing the results of the scan. To run a scan:

1. Download the tool package onto the server and unzip it. Double-click the Health Analyzer Tool if you are a member of the local Administrators group or right-click the tool and select **Run as administrator** to start this tool.
2. Configure the following three checkboxes on the interface.

   ***Note:** Each type of check detailed below can be run independently or simultaneously.

   - **Check Agent requirements on this server** – Configure the following settings to check the requirements of the Agent account for the selected modules.
     - **Username** – Enter the user name of the Agent account.
     - **Password** – Enter the password of the Agent account.

- **Module** – Select the modules that need to be checked from the drop-down list.

***Note:** By selecting this checkbox, the Stand-Alone Health Analyzer Tool will check the requirements of the Agent account for the current server.

- **Check Manager requirements on this server** – Configure the following setting to check the permissions of the application pool account.
  - **Username** – Enter the user name of the application pool account.
- **Check the connection on this server to other servers** – Configure the following settings to check the connection status from this server to other servers where you are about to install or have installed an Agent service, Control service, Media service, and/or Report service.
  - **Server IP/Hostname** – Enter the IP address or host name of the server where you are about to install or have installed an Agent service, Control service, Media service, and/or Report service.
  - **Server Port** – Enter the port number of the server where you are about to install or have installed an Agent service, Control service, Media service, and/or Report service.
  - Click **Add** to add this information into the table below. More than one set of server information can be added. Alternatively, click **Import Connections** to select a previously configured CSV file, and then click **Open** to import the server information in bulk. For more information on configuring the CSV file, refer to Configuring the CSV File for Importing the Server Information in Bulk. Click to delete a set of information from the table.

3. Click **Next** to go to the next page. The **Rules Selection** interface appears.
4. Select the rules that you want to scan by selecting the corresponding checkboxes and click **Scan** on the ribbon.
5. The results of the scan will show on the interface. Click the rule name, the **Rule Details** window will appear and show the explanation of the rule, the results, as well as the status and solution for the error. Click **Export Report** on the ribbon, select a desired storage location and click **Save** to export a Health Analyzer report to your local system.

## Configuring the CSV File for Importing the Server Information in Bulk

There is a template used to configure the server information for checking the connection status in the Health Analyzer tool package. Use the following steps to configure the CSV file:

1. Find the template file in the tool package.
2. Open the file, and enter the corresponding values under the **Server IP/Hostname** column and the **Server Port** column.
3. Save the changes to the file.

# 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 SP7 Agent host | Fundamental for all farms to be updated | Yes |
| Media service installed on each DocAve 6 SP7 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 Installation Wizard will guide you through the installation process. By following the steps below, you will have DocAve up-and-running on your environment very quickly. In order to complete the installation successfully, a local administrator must be used to run the Installation Wizard.

You need to install DocAve in the following order:

1. Install the DocAve Manager with the Manager Installation Wizard. DocAve does allow you to perform an unattended install for DocAve Manager. For more information refer to Appendix F: Unattended Installation of DocAve Manager.
2. Install the DocAve Agents with the Agent Installation Wizard. DocAve does allow you to perform an unattended install of Agents. For more information refer to Appendix G: Unattended Installation of DocAve Agent.
3. Log into DocAve to make sure the Manager and Agent are able to communicate with each other properly.

***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.

## DocAve Manager

Make sure the system requirements are met before starting installation for DocAve Manager. For more information, refer to the System Requirements for Control Service Installation, System Requirements for Media Service Installation and System Requirements for Report Service Installation sections of this guide.

***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 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.

### Installing DocAve Manager

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

## Installing DocAve Manager on Common Environments

DocAve Manager can be installed on the following environments.

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

To install DocAve Manager, complete the following steps:

***Note**: If you want to install DocAve Manager using the Built-in Database on a server running Windows Server 2003, Windows Installer 4.5 must be installed before you start the DocAve Manager installation. Click here to download and install Windows Installer 4.5.

1. Download the Manager ZIP file, either by requesting a demo version or by contacting an AvePoint representative for links to this package.
2. Extract 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 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 to display the scan result's detailed information. You can also click **Details** to view the detailed information of all the requirements.

   ***Note**: You cannot proceed the installation if any of the rules have a **Status** of **Failed**.

   - A **Failed** status means that your system does not meet the minimum requirement of the corresponding rule, and you must update your environment to meet the DocAve Manager system requirements. Click the **Rescan** button to check your environment again.
     - If any of the following rules fail, the **Fix** button is available to have the **DocAve Manager Installation Wizard** automatically update your environment to meet the rules: .NET Framework Features, .NET TCP Port Sharing Service, Windows Process Activation Service, World Wide Web Publishing Service, Web Server (IIS) Role, and IIS Admin Service. If the **Fix** button is available, you can have your environment automatically updated by clicking this button.
     - If any of the following rules fail, you must manually update your environment: Number of CPU Cores, Available Physical Memory, Available Disk Space, .Net Framework Version, and PowerShell Version.
   - If any of the rules have a **Warning** status, your system meets the minimum requirement of the corresponding rule but does not meet the recommended condition. In this case, you can still click **Next** to configure the **Control Service Configuration**.
   - If all of the rules are **Passed**, your system meets all of the recommended conditions in the DocAve Manager system requirements. Click **Next** to configure the **Control Service Configuration**.

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.

    ***Note**: AvePoint recommends using **MS SQL**, selecting **Built-in Database** will install the SQL Server Express that has a limitation in the size of the databases.

    - 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 **Start** > **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.

o **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** text box.

***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.

***Note**: When installing DocAve on a 32-bit system, you cannot use the **Built-in Database**.

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**: 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 **Install Completed** 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 **Install Completed** 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 **Use the previous database settings** or configure it yourself:

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

- Select the database type from the drop-down list, only MS SQL can be selected now.
    - **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 **Start** > **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 **Use the previous database settings** or configure it by yourself. 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**: The DocAve Auditor database should be created on a SQL server that does not store 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 amounts of disk space will be occupied when DocAve Compliance Reports fetches data from SharePoint content 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 **Start** > **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 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.

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.

      After the **User-defined Certificate** option is selected, click **Select Certificate** and a pop-up window will appear to display the certificates that meet the following requirements:
      - **Template**: Web Server or Subordinate Certification Authority

- **Enhanced Key Usage**: Server Authentication
- Make private key exportable: True
- **Key Type**: Exchange
- The certificate should be online.
- The certificate should have **Thumbprint** information
- The certificate should not be revoked or expired

Select a certificate and click **OK**.

If your local machine has certificates that meet the requirements, refer to Importing a Certificate.

If you do not have user-defined certificate, AvePoint provides a method for generating a certificate. For more detailed information, refer to Appendix E: User-defined Certificate.

***Note:** When creating a certificate for DocAve make sure that the certificate contains the **Friendly Name** field.

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. 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 improve technical support by sending DocAve usage feedback to AvePoint.
19. Click **Finish** to complete the installation and exit the installation wizard.

## Installing DocAve Manager on Windows Server 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core

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. Refer to the Generating the Installation Answer File for DocAve Manager section for more information.
2. Using the Command Line interface, change the current directory to the extracted DocAve Manager installation package.
3. Enter the following Manager installation command with the Answer file path and press **Enter** to start the DocAve Manager installation process.

```
Setup.exe Install-DocAveManager "Answer File Path"
```

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

## 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 Balancing cluster that use the same Control 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.
- Enter the Windows Network Load Balancing cluster's public IP address into the **Control Service Host** text box, and enter the hostname or IP address of the local host into the **Media**/**Report Service Host** text box when installing other DocAve Manager services.
- Enter the Windows Network Load Balancing cluster's public IP address into the **Control Service Host** text box, and enter the hostname or IP address of the local host into the **Agent Service Host** text box when installing DocAve Agents.
- Use the Windows Network Load Balancing cluster's 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 the jobs it carried out. For more information, refer to the DocAve 6 Job Monitor Reference Guide.

To install the DocAve Control service in a Windows Network Load Balancing cluster, complete the following steps:

1. Prepare the environment by configuring a Windows Network Load Balancing cluster containing two nodes: node **A** and node **B**.
    - The public IP address of this Windows Network Load Balancing cluster is **IP01**.
    - Node **A**'s IP address is **IP02**.
    - Node **B**'s IP address is **IP03**.
2. In the **Services Installation** step of DocAve 6 Manager for SharePoint Installation Wizard, select **Advanced** as the method. Then, select **Control Service**.
3. Install the DocAve Control service **Control01** on node **A**, configuring a common Control database named **ControlDB01** for this Control service loading balancing environment.

    Note the following:

a. In the **Control Service Configuration** step, enter **IP02** or node A's hostname in the **Control Service Host** field.

b. In the **Control Database Settings** step, enter the information of the common Control database **ControDB01** into the **Database Server** and **Control Database Name** fields.

c. In the **Passphrase** step, enter the passphrase you want to use for the Control database **ControlDB01** into the **Passphrase** field.

4. Install DocAve Control service **Control02** on node **B** using the same Control database **ControlDB01** as Control service **Control01**.

   Note the following:

   a. In the **Control Service Configuration** step, enter **IP03** or node **B**'s hostname in the **Control Service Host** field.

   b. In the **Control Database Settings** step, enter the database server and database name of the Control database **ControlDB01** into the **Database Server** and **Control Database Name** fields.

   c. In the **Passphrase** step, enter the passphrase used for Control database **ControlDB01** in step 3 into the **Passphrase** field.

5. According to your situation, choose one from the following methods to install the DocAve Media service and DocAve Report service. The Media service and Report service will use the Control service load balancing.

   - For best performance, install the DocAve Manager's services across multiple servers. To install the DocAve Media service and DocAve Report service on a server that does not have the DocAve Control service installed on it, complete the following steps:

     i. In the DocAve Manager installation package, double-click the **Setup.exe** file. The **DocAve 6 Manager for SharePoint Installation Wizard** appears.

     ii. In the **Services Installation** step, select **Advanced** as the method. Then, select **Media Service** and **Report Service**.

     iii. In the **Media Service Configuration** step, enter the public IP address **IP01** of the Windows Network Load Balancing cluster in the **Control Service Host** field.

     iv. In the **Report Service Configuration** step, enter the public IP address **IP01** of the Windows Network Load Balancing cluster in the **Control Service Host** field.

   - For a smaller environments, you can install the DocAve Manager's services on the same server. To install the DocAve Media service and DocAve Report service on node A and node B where the DocAve Control service resides, the server must meet all the system requirements for Manager's services. Refer to the DocAve Manager System Requirements for more details. If you choose this method, complete the following steps:

     i. In the DocAve Manager installation package, double-click the **Setup.exe** file. The **DocAve 6 Manager for SharePoint Uninstallation Wizard** appears.

ii. Select **Change** and click **Next**.

iii. In the **Service to Change** interface, select **Media Service** and **Report Service**, and then click **Next**.

iv. In the **Media Service Configuration** step, enter the public IP address **IP01** of the Windows Network Load Balancing cluster in the **Control Service Host** field.

v. In the **Report Service Configuration** step, enter the public IP address **IP01** of the Windows Network Load Balancing cluster in the **Control Service Host** field.

6. Install the DocAve Agent service on your desired servers.

   ***Note**: In the **Communication Configuration** step, enter the public IP address **IP01** of the Windows Network Load Balancing cluster in the **Control Service Host** field.

# DocAve Agent

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

Ensure that the following services are started before installing the DocAve Agent:

1. The DocAve Manager Control service that the DocAve Agent service will connect to.
2. The Windows Management Instrumentation service on the server where you will install the Agent.

## Installing DocAve Agents

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

### Installing DocAve Agent on Common Environments

DocAve Agent can be installed on the following common Windows environments:

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

After the DocAve Manager's Control service that the Agent service will connect to 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. Extract 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 languages.

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 to view the scan result's detailed information, or click **Details** to view the detailed information on all of the requirements.

   ***Note**: You cannot proceed the installation if the **Status** of any of the rules is **Failed**.

   - A **Failed** status means that your system does not meet the minimum requirement of the corresponding rule, and you must update your environment to meet the DocAve Agent system requirements. Click the **Rescan** button to check your environment again.
     - If any of the following rules fails, the **Fix** button is available to have the **DocAve Agent Installation Wizard** automatically update your environment to meet the rules: .NET Framework Features and .NET TCP Port Sharing Service. If the **Fix** button is available, you can have your environment automatically updated by clicking this button.
     - If any of the following rules fails, you must manually update your environment to meet the rules: Number of CPU Cores, Available Physical Memory, Available Disk Space, .Net Framework Version, and PowerShell Version.
   - If the status of any rule is **Warning**, your system meets the minimum requirement of the corresponding rule, but does not meet the recommended condition. In this case, you can still click **Next** to configure the **Communication Configuration**.
   - If all of the rule statuses are **Passed**, your system meets all of the recommended conditions in the DocAve Agent system requirements. Click **Next** to configure the **Communication Configuration**.

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 that can communicate with the current 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).
   - **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.

  After the **User-defined Certificate** option is selected, click **Select Certificate** and a pop-up window will appear to display the certificates that meet the following requirements:

  - **Template**: Web Server or Subordinate Certification Authority
  - **Enhanced Key Usage**: Server Authentication
  - Make private key exportable: True
  - **Key Type**: Exchange
  - The certificate should be online.
  - The certificate should have **Thumbprint** information
  - The certificate should not be revoked or expired

  ***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.

  Select a certificate and click **OK**.

  If your local machine has certificates that meet the requirements, refer to Importing a Certificate.

  If you do not have user-defined certificate, AvePoint provides a method for generating a certificate. For more detailed information, refer to Appendix E: User-defined Certificate.

  ***Note:** When creating a certificate for DocAve make sure that the certificate contains the **Friendly Name** field.

Click **Next**.

9. Set up the **Agent Configuration**:
   - **Agent Authentication** – Enter the Manager Passphrase entered during 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** > **Security Information** > **Manage Passphrase**. For more information, refer to the DocAve 6 Control Panel Reference Guide.

- **Agent Account** – Specify the Agent account that will perform Agent activities. 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 in Appendix D: Permission Requirements for DocAve Modules.

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.

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 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core

Once the Manager 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. Refer to the Generating the Installation Answer File for DocAve Agent section for more information.
2. Using the Command Line interface, change the current directory to the extracted DocAve Agent installation package.
3. Enter the Agent installation command with the Answer file path and press **Enter** to start the DocAve Agent installation process.

   ```
   Setup.exe Install-DocAveAgent "Answer File Path"
   ```

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

# Accessing the DocAve GUI

DocAve 6 can be installed and accessed in an 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 by completing the following steps:

1. To first access the login page of DocAve Manager on the Manager server (where the DocAve Control service is installed), choose one of the following methods:
    - Double-click the **DocAve 6 Manager for SharePoint** shortcut on the desktop.
    - Navigate to **Start** > **All Programs** > **AvePoint DocAve 6**. Click **DocAve 6 Manager for SharePoint**.
    - Go to the **Control** folder in the *…/AvePoint/DocAve6/Manager/* directory and run the **shortcut.html** file.

    The IE window used for accessing the login page of DocAve Manager appears.

2. The IE window displays a security certificate prompt:

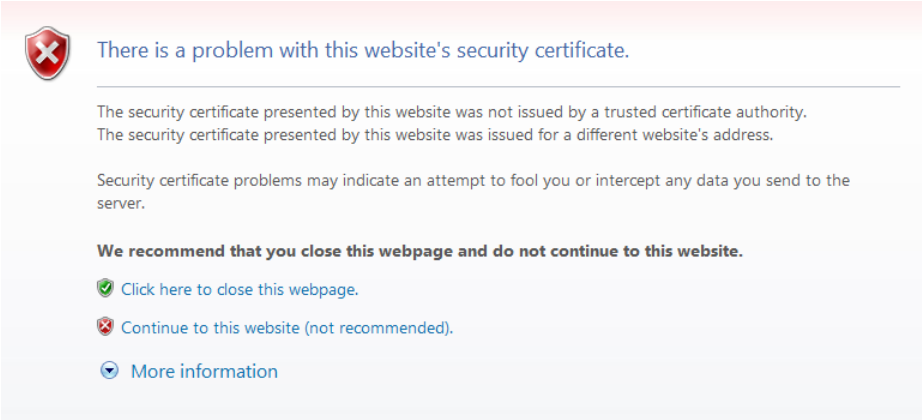



**Figure 1: The security certificate prompt displayed by the IE window.**

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

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

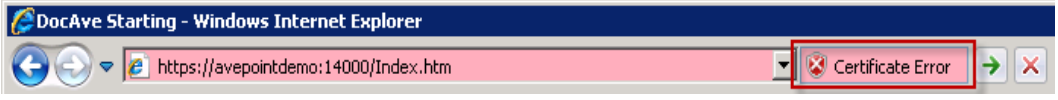



**Figure 2: Clicking the Security Report icon next to the address URL.**

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

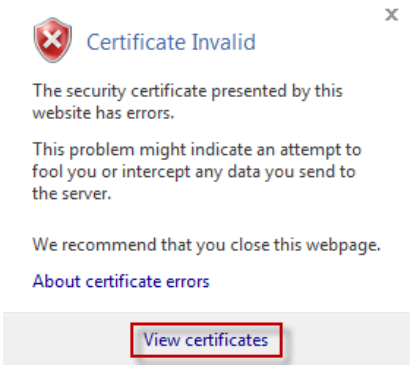



**Figure 3: Clicking View certificates in the pop-up.**

5. 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.

**Figure 4: Clicking the Install Certificate… button to install DocAve certificate.**

6. Click **Next** to continue with the **Certificate Import Wizard**.
7. 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**.

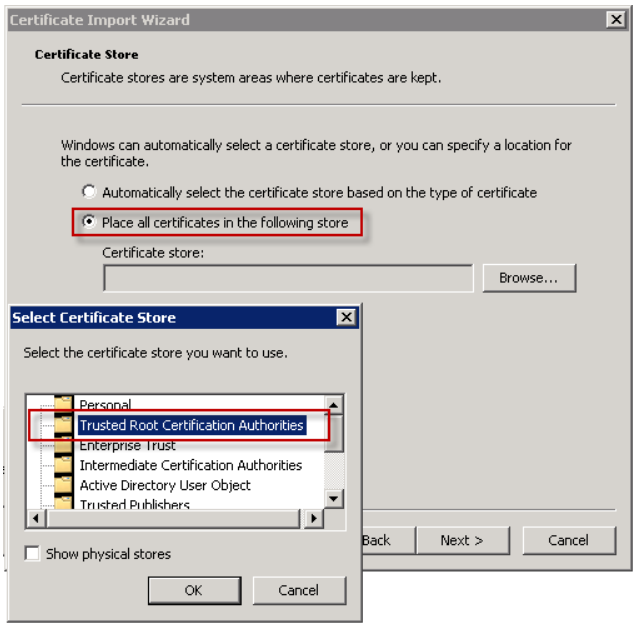



**Figure 5: Importing the DocAve certificate using the Certificate Import Wizard.**

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

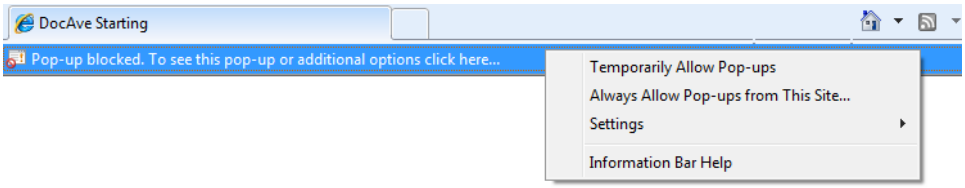



**Figure 6: Selecting temporarily allow popping up the DocAve GUI or always allow in the security prompt.**

Now you can log into DocAve from Internet Explorer.

## Modifying SSL Certificate of DocAve6 Website

If you want to modify the SSL certificate of DocAve6 Website, follow the steps below.

1. On the machine with the DocAve Manager installed, open the Internet Information Services (IIS) Manager.
2. Select DocAve6 under the **Sites** node.
3. Click **Bindings…** and the **Site Bindings** window appears.
4. Select the site and click **Edit**. The **Edit Site Binding** window appears.
5. Select a certificate from the **SSL certificate**, and click **OK**.

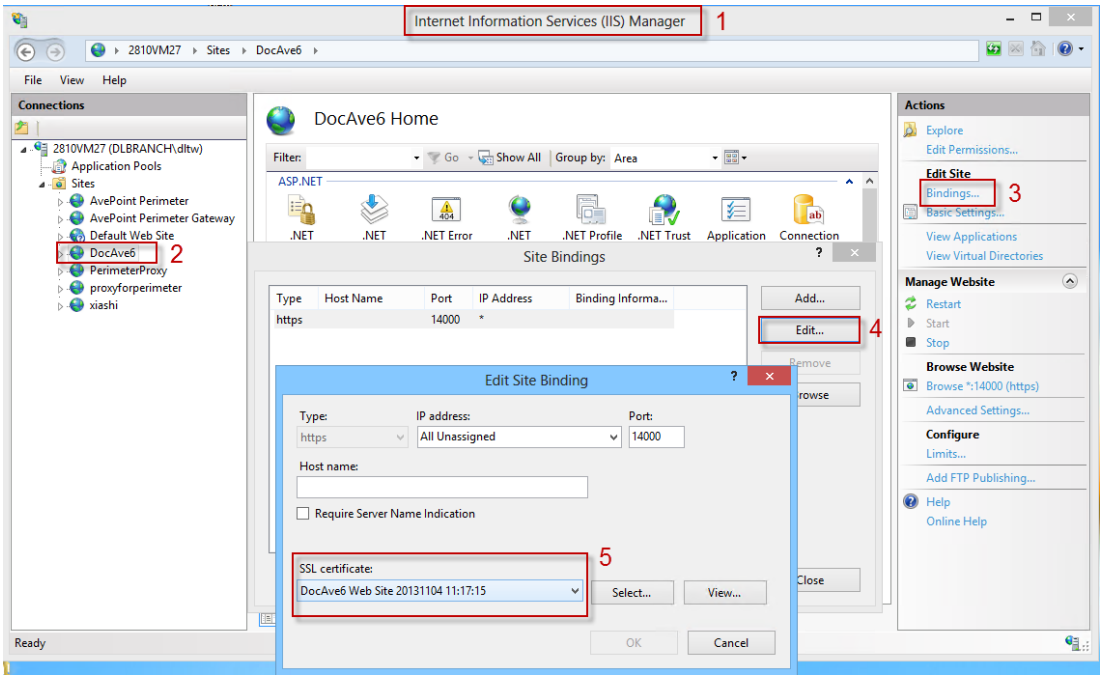



**Figure 7: Modifying SSL certificate of DocAve6 Website.**

# 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**: If this is your first time logging into the DocAve 6 Manager on the Azure VM, the **DocAve License Agreement** window appears after you enter the login ID and the password. After

carefully reading the DocAve License Agreement, check the **I have read the terms in the license agreement** checkbox and click **Accept** to log into DocAve 6 Manager.

***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.

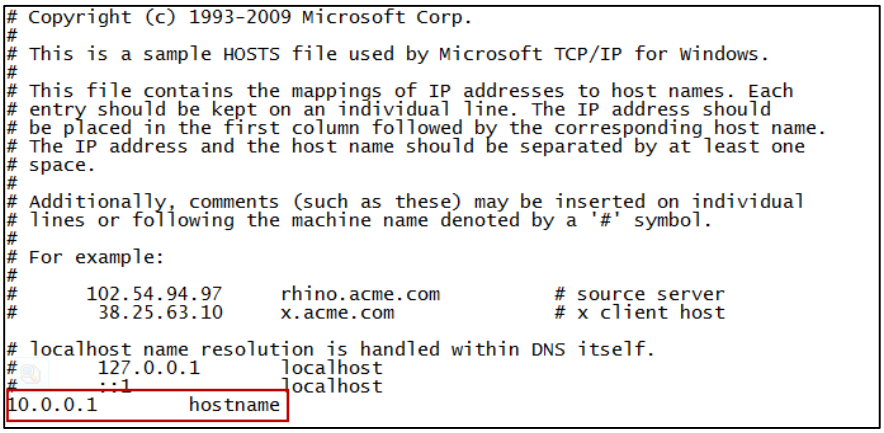
# Out-of-Browser Accessing DocAve Manager

DocAve Manager can be installed as a shortcut on the local machine when remotely accessing the DocAve Manager. Follow the instructions below to perform Out-of-Browser (OOB) installation.

***Note**: The Out-of-Browser (OOB) installation can be performed only when the shortcut for DocAve Manager is available on the server where DocAve Control service is installed.

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 built-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 built-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.

# After You Install DocAve

After you install DocAve, it is important to configure DocAve Health Analyzer scans to regularly check your environment. Changes in different parts of your environment can affect DocAve, and configuring DocAve Health Analyzer profiles is a pre-emptive step that will help you notice, troubleshoot, and fix potential problems specifically related to prerequisite connection, permissions, services and more.

## DocAve Health Analyzer Best Practices

DocAve Health Analyzer is a tool that scans the DocAve environment and farms to report any issues that may affect the DocAve modules. AvePoint recommends several best practices that should be followed to help ensure a healthy DocAve environment.

1. Create a DocAve Health Analyzer profile to scan each farm that requires regular monitoring. Be sure to set up a profile for your Production farm.
2. Create a schedule for each profile that scans the environment on a regular basis and before major DocAve jobs, especially Backup jobs. Running a scan before major DocAve jobs, such as a Backup, can provide pre-emptive, pin-point troubleshooting of the job.
3. Create e-mail notifications for DocAve Health Analyzer jobs to notify you of job results. Setting up e-mail notifications will make it so you don't need to log into the DocAve interface to check the status of Health Analyzer jobs.
4. If a DocAve Health Analyzer scan reports a rule error—such as an Agent connection problem—fix the issue, according to the DocAve Health Analyzer rules' details, and run the scan again to confirm that the problem has been resolved.

## DocAve Health Analyzer

DocAve Health Analyzer scans the farm according to rules you select in the Health Analyzer profiles to report on connection, permission, service and other issues that may affect DocAve modules. The DocAve Health Analyzer, however, does not report on port configuration issues, which can be discovered using the Stand-Alone Health Analyzer.

***Note:** Only the users in the DocAve **Administrators** group can use DocAve Health Analyzer.

DocAve Health Analyzer provides rules in four categories regarding the health of the DocAve modules.

- **Connection** – Checks the connectivity among DocAve services.
- **Permission** – Verifies appropriate permissions for the Agent account and the DocAve application pool account.
    - **Local System Permission** – Verifies appropriate permissions of the local system.
    - **SharePoint Permission** – Verifies appropriate permissions of the SharePoint.

    - **SQL Permission** – Verifies appropriate permissions of the SQL.
- **Service** – Checks the status of DocAve services.
- **Others** – Verifies that all of the requirements for each module are met.

To use DocAve Health Analyzer to check the health of the DocAve modules, complete the following procedures:

1. Create a DocAve Health Analyzer profile to include the rules you are about to scan for the DocAve modules. For more information, refer to Creating a DocAve Health Analyzer Profile.
2. Run the newly created profile.
3. After the job is finished, check the status of the rules in the profile. If the status is **Warning** or **Error**, click the rule to view the provided solution. For more information, refer to Managing Rules in a DocAve Health Analyzer Profile.
4. Solve the issue according to the provided solution.

You can also re-scan the rules, after you have solved the issue, to ensure that the provided solution solved the problem.

From the **DocAve** tab, click **Health Analyzer** to launch the Health Analyzer. Alternatively, you can click the Health Analyzer ( ) button from anywhere within the DocAve software to launch **Health Analyzer**.

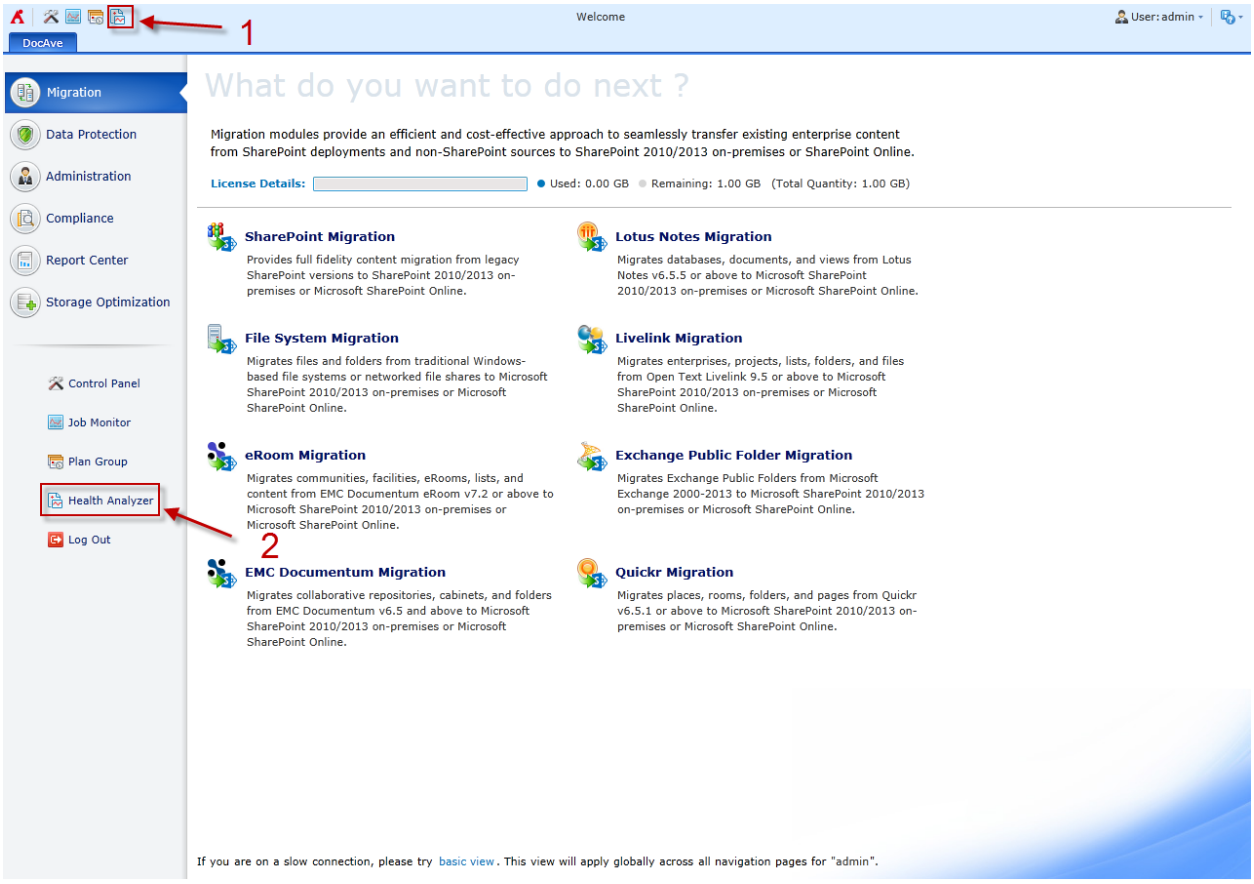



**Figure 8: Launching Health Analyzer.**

# Managing DocAve Health Analyzer Profiles

In the **Health Analyzer** interface, click **Profile Manager** on the ribbon. In the **Profile Manager** interface, you will see a list of previously configured profiles. In the **Profile Manager** interface, you can perform the following actions to the profiles:

- **Create** – Creates a profile. To do so, click **Create** on the ribbon.
- **View Details** – Views the detailed information of the selected profile. To do so, select a profile by selecting the corresponding checkbox, and then click **View Details** on the ribbon.
- **Edit** – Edits the selected profile. To do so, select a profile by selecting the corresponding checkbox, and then click **Edit** on the ribbon.
- **Delete** – Deletes the selected profiles. To do so, select one or more profiles by selecting the corresponding checkboxes, and then click **Delete** on the ribbon.

- **Run Now** – Run the selected profile immediately. To do so, select a profile by selecting the corresponding checkbox, and then click **Run Now** on the ribbon.
- **Job Monitor** – View and manage the profiles' jobs. To do so, click **Job Monitor** on the ribbon.

A default profile is created automatically after the installation or upgrade. This profile will be run at midnight (00:00:00) every Monday and includes all of the existing Agents, modules and rules. If you have a profile named "Default Profile" before upgrading to the DocAve 6 Service Pack 5, your profile will be renamed as "Default Profile-1" after the upgrade in order to discriminate it from the default profile created automatically here. The original name and the reason why it was renamed is written in the description of the renamed profile.

## Creating a DocAve Health Analyzer Profile

In the **Profile Manager** interface, click **Create** on the ribbon to create a new Health Analyzer profile. Complete the following steps to create a new profile:

1. **Profile Name** – Enter a name for your profile, and then enter an optional description for future reference. Click **Next**.
2. **Scan Filter** – Filters the modules and the Agents whose health you want to check.
    - **Module Filter** – Select one or more modules that you want to scan.

      ***Note**: **Cloud Connect** module and **Connector** module share the same scanning rules, so select **Connector** in the Health Analyzer **Module Filter** settings to scan the environment for **Cloud Connect**.

    - **Agent Filter** – Select one or more Agents that you want to scan.
        - **Include New** – Includes newly registered or restarted Agent services when scanning all of the available rules.

          ***Note:** The rules used to scan the newly included Agent services are the same as those selected when saving the Health Analyzer profile.

        - **Agents** – Displays all of the Agents that are installed in the corresponding farm.
        - **Non-SharePoint Agents** – Displays all of the Agents that are installed on servers without SharePoint installed.
3. Click **Next** to proceed.
4. **Scan Rules** – Select the rules you want to include in your profile. When running the newly created profile, DocAve checks all of the rules included in the profile.
5. Click **Next** to proceed.
6. **Scan Schedule** – Configure the scan schedule and notification settings for your profile.
    - **Schedule** – Select one of the following options:

    - **No schedule** – Scans the rules included in the profile only when you run the profile.
    - **Configure the schedule myself** – Scans the rules included in the profile according to the customized schedule settings. If you select this checkbox, the **Scan Schedule** field will appear. For more information, refer to Configuring Scan Schedule Settings for the DocAve Health Analyzer Profile.

- **Notification** – Select an existing notification profile from the drop-down list or click **New Notification Profile** to create a new one. After selecting the notification profile, click **View** to view more details of this profile.
- **Notification Settings** – Select when to receive the notification e-mail.
    - **Passed** – You will receive a notification e-mail with a report that includes all of the rules that have a **Passed** status.
    - **Warning** – You will receive the report including all of the rules that are in **Warning** status through the notification e-mail.
    - **Error** – You will receive a notification e-mail with a report that includes all of the rules that have an **Error** status.
    - **Skipped** – You will receive a notification e-mail with a report that includes all of the rules that have a **Skipped** status.
    - **Stopped** – You will receive a notification e-mail with a report that includes all of the rules that have a **Stopped** status.
    - **Unscanned** – You will receive a notification e-mail with a report that includes all of the rules that have an **Unscanned** status.

7. Click **Next** to proceed.
8. **Overview** – View the detailed information of your profile.
9. Click **Finish** to save the profile, or click **Finish and Run Now** to save and run the profile.

## Configuring Scan Schedule Settings for the DocAve Health Analyzer Profile

In the **Scan Schedule** field, after selecting the **Configure the schedule myself** checkbox, click the **Add Schedule** link to add a new schedule for the profile. The **Add Schedule** interface appears. Complete the following steps to configure the scan settings:

1. **Type** – Select a type of recurring schedule for the schedule you want to add from the following four options:
    - By hour
    - By day
    - By week
    - By month
2. **Schedule Settings** – Select how frequently the recurring schedule is run:

- **Every _ hours** – Enter a positive integer in the text box. This option appears when you select **By hour** in the **Type** field. Select **Advanced** to configure more specific settings:
    - **Specify production time** – Select the start hour and the end hour in this field.
    - **Select time below** – Select when you will scan the rules. Click **Add** to add more times.
- **Every _ day(s)** – Enter a positive integer in the text box. This option only appears when you select **By day** in the **Type** field.
- **Every _ week(s)** – Enter a positive integer in the text box. This option only appears when you select **By week** in the **Type** field. Select **Advanced** to configure more specific settings:
    - **Run every _ week(s)** – Enter a positive integer in the text box.
    - **On _** – Select one or more options from the drop-down list, and then click **OK**.
- **Every _ month(s)** – Enter a positive integer in the text box. This option appears when you select **By month** in the **Type** field. Select **Advanced** to configure more specific settings:
    - **On day _ of _** – Enter a positive integer in the text box, and then select one or more month from the drop-down list.
    - **Day_ of every _ month(s)** – Select a day from the drop-down list, and then enter a positive integer in the text box.
    - **The _ _ of every _ month(s)** – Select an ordinal numeral from the first drop-down list, select one or more day from the second drop-down list, and then enter a positive integer in the text box.
    - **The _ _ of _**– Select an ordinal numeral from the first drop-down list, select one or more days from the second drop-down list, and then select one or more months from the third drop-down list.

3. **Range of Recurrence** – Select when the recurring schedule will end:
    - **Start time** – Select a start time.
    - **No end date** – The schedule will not end.
    - **End after _ occurrences** – Enter a positive integer in the text box. The schedule will end after the entered number of occurrences.
    - **End by _** – Select the end date. The schedule will end on the selected end date.
4. Click **Save** to save your changes and return to **Scan Schedule** interface or click **Cancel** to return to **Scan Schedule** interface without saving any changes.
5. Click **Add Schedule** to add more schedules for your profile.
6. Click **Calendar View** to view the overall schedules.

## Managing Rules in a DocAve Health Analyzer Profile

In the **Health Analyzer** interface, you can perform the following actions:

- **Profile Manager** – Manages all of the Health Analyzer profiles. For more information, refer to Managing DocAve Health Analyzer Profiles.
- **Export Report** – Exports a report for all of the rules in the selected profile.
- **View Details** – Views the detailed information of the selected rule. Select a rule and then click **View Details** on the ribbon.
- **Stop Scanning** – Stops scanning the selected rules. Select one or more rules and then click **Stop Scanning** on the ribbon.
- **Rescan** – Rescans the selected rules. Select one or more rules and then click **Rescan** on the ribbon.
- **Job Monitor** – Monitors all of the Health Analyzer jobs.

## Exporting DocAve Health Analyzer Report

To export a DocAve Health Analyzer report, which will allow you to view detailed information about the rules included in a profile, complete the steps below:

1. In the **Health Analyzer** interface, select a profile from the **Profile Name** drop-down list.
2. Select a collection time from the **Collection Time** drop-down list. By default, the latest collection time of the selected profile is displayed.
3. To export all of the scan results, click **Export Report**. To export particular scan results, select the checkboxes of the rules you want to export and click **Export Report**.
4. Click **Export Report** on the ribbon to export a Health Analyzer report. The **Export Report** interface appears.
5. In the **Scan Results Selection** field, choose to export all of the scan results or only the selected scan results.
6. Select a report format from the **Select a report format** drop-down list in the **Report Format** field.
7. Click **OK**. The report will be exported to a location you specified.

# DocAve Manager and Agent Maintenance

## Using the DocAve Manager/Agent Configuration Tool

If the database type is MS SQL, you can change the Control database, Auditor database, and/or Report database to another existing Control database, Auditor database, or Report database using DocAve Manager Configuration Tool. To modify the configuration of the DocAve Manager or Agent after the installation, use one of the following methods to access the DocAve Manager or Agent Configuration Tool.

- Open the **Start Menu** in Windows on the DocAve Manager/Agent server, and refer to the navigations below according to your server's operating system:
    - For the server with the Windows Server 2012/2012 R2 or later version installed, navigate to **Start** > **Apps**, and click **Manager Configuration Tool**/**Agent Configuration Tool**.
    - For the server with the operating system earlier than Windows Server 2012/2012 R2 is installed, navigate to **All Programs** > **AvePoint DocAve 6** > **DocAve Manager Tools**/**DocAve 6 Agent Tools**, and click **Manager Configuration Tool**/**Agent Configuration Tool**.
- Run the **DocAve Manager**/**Agent Configuration Tool** by running the application file directly in the installation directory on DocAve Manager or Agent server.
    - To run the DocAve Manager Configuration Tool, go to the **Uninstall** folder in the *…/AvePoint/DocAve6/Manager/* directory on the Manager server and run the **ManagerToolConfiguration.exe** application file.
    - To run the DocAve Agent Configuration Tool, go to the **Uninstall** folder in the *…/AvePoint/DocAve6/Agent/* directory on the Agent server and run the **AgentToolConfiguration.exe** application file.

In the DocAve Manager/Agent Configuration Tool interface, click the items listed on the navigation pane and you can modify the corresponding settings.

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

***Note**: You must enter the passphrase 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

To restart the services of DocAve Manager or Agent after the installation, use either of the following two methods to access the DocAve Manager/Agent Restart Service Tool.

- Open the **Start Menu** in Windows on the DocAve Manager/Agent server, and refer to the navigations below according to your server's operating system:
    - For the server with the Windows Server 2012/2012 R2 or later version is installed, navigate to **Start** > **Apps**, and click **Manager Restart Service Tool**/**Agent Restart Service Tool**.
    - For the server with the operating system earlier than Windows Server 2012/2012 R2 is installed, navigate to **All Programs** > **AvePoint DocAve 6** > **DocAve 6 Manager Tools**/**DocAve 6 Agent Tools**, and click **Manager Restart Service Tool**/**Agent Restart Service Tool**.
- Run the DocAve Manager/Agent Restart Service Tool by running the application file directly in the installation directory on DocAve Manager/Agent server.
    - To run the DocAve Manager Restart Service Tool, go to the **Uninstall** folder in the *…/AvePoint/DocAve6/Manager/* directory on the Manager server and run the **ManagerToolRestartService.exe** application file.
    - To run the DocAve Agent Restart Service Tool, go to the **Uninstall** folder in the *…/AvePoint/DocAve6/Agent/* directory on the Agent server and run the **AgentToolRestartService.exe** application file.

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 any of the three methods below to access the uninstallation wizard of DocAve Manager/Agent on the Manager/Agent server 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.

- Open the Start Menu in Windows on the DocAve Manager/Agent server and navigate to All Programs > AvePoint DocAve 6 > DocAve 6 Manager Tools/DocAve 6 Agent Tools. Click Manager Uninstall/Agent Uninstall.
- Double click the **Setup.exe** file in the extracted folder of the DocAve Manager/Agent installation package and run it.

- Run the uninstallation wizard of DocAve Manager/Agent by running the application file directly in the installation directory on the DocAve Manager/Agent server.
    - To run the uninstallation wizard for DocAve Manager, go to the **Uninstall** folder in the *…/AvePoint/DocAve6/Manager/* directory on the Manager server and run the **ManagerUnisntallation.exe** application file.
    - To run the uninstallation wizard for DocAve Agent, go to the **Uninstall** folder in the *…/AvePoint/DocAve6/Agent/* directory on the Agent server and run the **AgentUnisntallation.exe** application file.

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

## Changing 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.

## Repairing 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 Manager 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

Before uninstalling Connector, perform the following steps on the SharePoint libraries where Connector stubs exist:

If using **SharePoint Built-in Libraries**, you can move the original content from the storage device into SharePoint. Use either of the following two methods to deal with the Connector stubs stored in **SharePoint Built-in Libraries**:

To move the original content to SharePoint:

1. Perform a **Convert Stub to Content** job on the SharePoint built-in libraries.
2. Delete **Connector Settings** in the corresponding library settings.

For more information on how to perform these actions, refer to the **Converting Stubs to Content** and **Removing Connector Settings** sections in the Connector User Guide.

If you do not want to move the original content into SharePoint, remove the **Connector Settings** in the corresponding library. This will delete the stubs in the library, and the original content will still exist in the storage device. For more information, refer to the **Removing Connector Settings** section in the Connector User Guide.

1. **Connector Libraries** will be inaccessible after the Connector solutions are uninstalled. Before uninstalling Connector, perform the following steps on the Connector Libraries:
2. Remove the **Connector Settings** in the **Connector Libraries** (refer to the **Removing Connector Settings** section in the Connector User Guide).
3. Delete the Connector Libraries.
4. Uninstall the Connector solutions from your SharePoint farm (refer to the **Operations on the Solutions** section in the Control Panel User Guide).

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

## Cloud Connect

Before uninstalling Cloud Connect, perform the following steps on the SharePoint libraries where Cloud Connect stubs exist:

If using **SharePoint Built-in Libraries**, you can move the original content from Box into SharePoint. Use either of the following two methods to deal with the Cloud Connect stubs stored in **SharePoint Built-in Libraries**:

To move the original content into SharePoint:

1. Perform a **Convert Stubs to Content** job on the SharePoint built-in libraries.
2. Delete **Cloud Connect Settings** in the corresponding library settings.

For details on how to perform these actions, refer to the **Converting Stubs to Content** and **Removing Cloud Connect Settings** sections in the Cloud Connect User Guide.

If you do not want to move the original content into SharePoint, remove the **Cloud Connect Settings** in the corresponding library. This will delete the stubs in the library and the original content will still exist in Box. For more information, refer to the **Removing Cloud Connect Settings** section in the Cloud Connect User Guide.

**Cloud Connect Libraries** will be inaccessible after the Cloud Connect solutions are uninstalled. Before uninstalling Cloud Connect, perform the following steps on the Cloud Connect Libraries:

1. Remove the **Cloud Connect Settings** in the **Cloud Connect Libraries** (refer to the **Removing Cloud Connect Settings** section in the Cloud Connect User Guide).
2. Delete the Cloud Connect libraries.
3. Uninstall the Cloud Connect solutions from your SharePoint farm (refer to the **Operations on the Solutions** section in the Control Panel Reference Guide).

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

# Uninstalling DocAve Manager

In order to uninstall DocAve Manager, please ensure the Manager services being removed are not in use by another process.

## Uninstalling DocAve Manager from Common Environments

The section below offers the instructions on uninstalling DocAve Manager from the following common Windows environments:

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

To uninstall DocAve Manager, complete the following steps:

1. Go to the server from which you want to uninstall the Manager services.
2. Access the uninstallation wizard using a method provided in Using the DocAve Manager/Agent Uninstallation Wizard.
3. In the DocAve 6 Manager for SharePoint Uninstallation Wizard interface, select the Remove option. Click Next.
4. In the **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 Settings** > **System Options** > **Security Settings** > **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 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core

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

1. Change the directory to the extracted 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 Agents

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

### Uninstalling DocAve Agent from Common Environments

The section below offers the instructions on uninstalling DocAve Agents from the following common Windows environments:

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

To uninstall DocAve Agent, complete the following steps:

1. Go to the server from which you want to uninstall the DocAve Agent.
2. Access the uninstallation wizard using a method provided in Using the DocAve Manager/Agent Uninstallation Wizard.
3. In the DocAve 6 Agent for SharePoint Uninstallation Wizard interface, 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. If there are running jobs or processes on the machine when the Agent is removed, a pop-up window appears. Click **View Details** in the pop-up window to view the detailed information about the running jobs and processes. Click **OK** to proceed with the uninstallation, or click **Cancel** to go back to the **Ready to Remove DocAve 6 Agent** interface.
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 2008 R2 SP1 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core

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 extracted 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, Cloud Connect, and Replicator.

## Modifying the Port Used by DocAve Storage Manager, Connector and Cloud Connect

If the default port (14005) used by DocAve Storage Manager, Connector, and Cloud Connect is occupied by another application on a DocAve Agent server, you can go to the related directory according to your SharePoint version and modify the following configuration file to change the port:

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

To change the port used by DocAve Storage Manager, Connector, and Cloud Connect, complete the following steps:

1. Navigate to the *…\AvePoint\DocAve6\Agent\data\SP2010\Arch* directory on the DocAve Agent server.
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.

## Modifying the Port Used by DocAve Replicator

If the default port (14006) used by DocAve Replicator is occupied by another application on a DocAve Agent server, you can modify the following configuration file to modify the port:

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

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

1. Navigate to the *…\AvePoint\DocAve6\Agent\data\SP2010\Replicator* directory on the DocAve Agent server.
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.

# Modifying the Port Used by DocAve High Availability

If the default port (14007) used by DocAve High Availability for data transfer is occupied by another application on a DocAve Agent server, you can modify the following configuration file to change the port: *…\AvePoint\DocAve6\Agent\data\HighAvailability\AgentCommonHAConfiguration.xml* on each DocAve Agent server.

To change the port used for DocAve High Availability data transfer, complete the following steps:

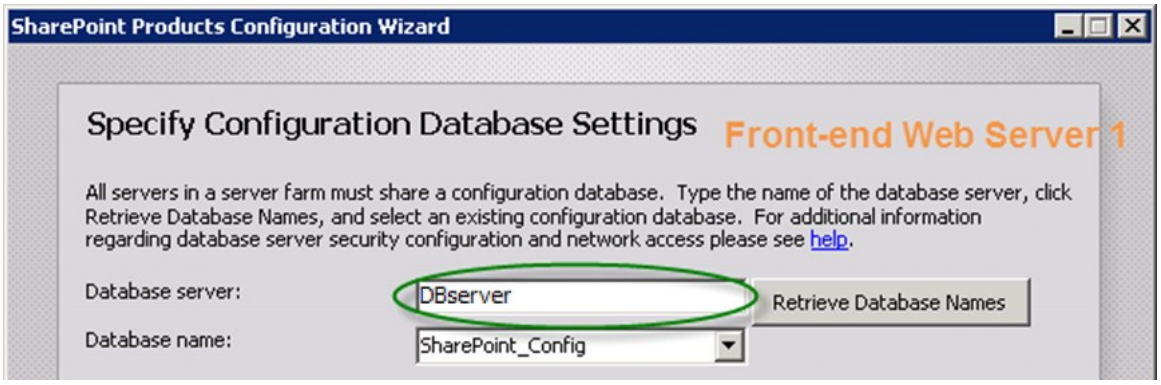
1. Go to the *…\AvePoint\DocAve6\Agent\data\HighAvailability* directory on the each DocAve Agent server.
2. Find the **AgentCommonHAConfiguration.xml** file, and open it with Notepad.
3. Modify the value of **SendDataPort** to an available port.
4. Save the configuration file.
5. Start the Task Manager on the Agent where destination SQL Server resides to end the **AgentCommonHADataTransferServices.exe** process.

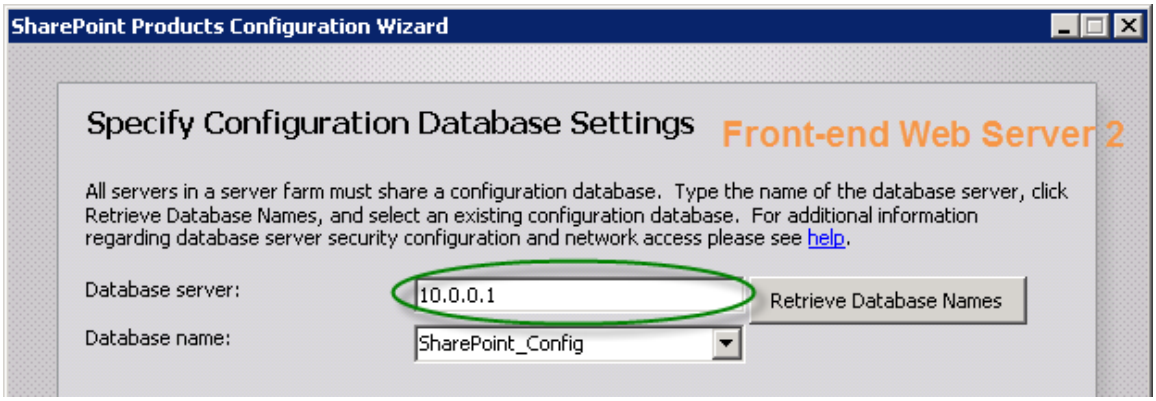
# Helpful Notes

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 the 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 the 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 that 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 Server and configure the following settings according to the steps below:

1. Log into SQL Server instance 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 2007 to 2016 Migration | Source: SharePoint 2007 | DocAve Agent must be installed on at least one of the source Web front-end servers. |
| | | Destination: SharePoint 2016 | 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. |
| | SharePoint 2010 to 2016 Migration | Source: SharePoint 2010 | DocAve Agent must be installed on at least one of the source Web front-end servers. |
| | | Destination: SharePoint 2016 | DocAve Agent must be installed on at least one of the destination Web front-end servers. |
| | SharePoint 2013 to 2016 Migration | Source: SharePoint 2013 | DocAve Agent must be installed on at least one of the source Web front-end servers. |
| | | Destination: SharePoint 2016 | 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 a Lotus Notes client installed. |

| 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. |
| | Quickr Migration | Source: Quickr | DocAve Agent must be installed on the server with a 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. |
| | File System Migration | Source: File System | DocAve Agent must be installed on at least one of the servers that are able to access the File System server where you want to perform migration. If the destination SharePoint Web front-end server is able to access the source File System server, the DocAve Agent installed on the destination SharePoint Web front-end server can be used as both source and destination Agent for File System Migration. |
| | | Destination: SharePoint 2010 SharePoint 2013 SharePoint 2016 | 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:<br>• .Net Framework 3.5.1<br>• Microsoft Visual J# Version 2.0 |
| | | Destination: SharePoint 2010 SharePoint 2013 SharePoint 2016 | 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. |

| Product Suites | Product | | Detailed Places to Install DocAve Agents |
|---|---|---|---|
| | | Destination: SharePoint 2010 SharePoint 2013 SharePoint 2016 | 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.<br>If the MAPI access method is used in the Exchange Public Folder connection, DocAve Agent must be installed on the server with Microsoft Outlook (32-bit) installed and the server must be able to access the server with Exchange installed.<br>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 SharePoint 2016 | 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 install the **Documentum DFC Runtime Environment** program. |
| | | Destination: SharePoint 2010 SharePoint 2013 SharePoint 2016 | 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:<br>• DocAve Agent must be installed on at least one of the Web front-end servers. |

| Product Suites | Product | Detailed Places to Install DocAve Agents |
|---|---|---|
| | | • The Search Service Application server where you want to back up the components of the specified Search Service Application.<br>• The SharePoint Foundation (Help) Search server where you want to back up the components of the SharePoint Foundation (Help) Search.<br>• 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.<br>• Each FAST Search server where you want to back up the FAST Search server settings.<br>• The server installed with Microsoft SQL Server containing the SharePoint databases, DocAve stub databases, and the databases of the DocAve-supported third-party applications you want to back up.<br>• Each node of Microsoft SQL Cluster.<br>***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, enter the name of local SQL server into text box of DocAve Agent Host. |

| Product Suites | Product | | Detailed Places to Install DocAve Agents |
|---|---|---|---|
| | | | • Each replica of the Microsoft SQL **AlwaysOn Availability Groups** if you are using SQL Server 2012<br>• 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.<br>• To perform a Farm Rebuild, install DocAve Agent on each server in the SharePoint farm (including all of the SharePoint servers and SQL servers).<br>• To Perform a Farm Clone, install DocAve Agent on each server in the destination 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:<br>• 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.<br>• All of the SQL servers where the SharePoint databases reside.<br>***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.<br>• Each node of Microsoft SQL Cluster.<br>• Each replica of the **AlwaysOn Availability Group** where you will perform the High Availability jobs with **AlwaysOn Availability Group** method.<br>***Note**: DocAve recommends installing |

| Product Suites | Product | Detailed Places to Install DocAve Agents |
|---|---|---|
| | | the DocAve Agent on each replica of the Microsoft SQL **AlwaysOn Availability Groups**, if you are using SQL Server 2012. |
| | VM Backup & Restore | • To back up and restore Hyper-V VMs, DocAve must be installed on the Hyper-V host server.<br>• To back up and restore VMs on Hyper-V host server that is in the failover cluster, DocAve must be installed on each node of the failover cluster.<br>• To back up and restore ESX/ESXi or vCenter VMs, the DocAve Agents must be installed on the servers or computers (64-bit Windows operating system) that are able to connect to the specific ESX/ESXi or vCenter host server. |
| Administration | Administrator<br>Content Manager<br>Deployment Manager | DocAve Agent must be installed on at least one of the Web front-end servers.<br>***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 Web front-end servers.<br>***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.<br>• 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.<br>***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. |

| Product Suites | Product | Detailed Places to Install DocAve Agents |
|---|---|---|
| Storage Optimization | Real-Time/Scheduled Storage Manager(In RBS environment) | • DocAve Agents must be installed on all the Web front-end servers.<br>• 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.<br>• 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 Web front-end servers.<br>• 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.<br>• 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.<br>• 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 |

| Product Suites | Product | Detailed Places to Install DocAve Agents |
|---|---|---|
| | | Application and Excel Calculation Services.<br>• 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 Web front-end servers.<br>• 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.<br>• 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. |
| | Cloud Connect (In RBS environment) | • DocAve Agents must be installed on all the Web front-end servers.<br>• 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.<br>• 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 |

| Product Suites | Product | Detailed Places to Install DocAve Agents |
|---|---|---|
| | | DocAve Agent on the server which installs the add-in |
| | Cloud Connect (In EBS environment) | • DocAve Agents must be installed on the SharePoint Central Administration server and all the Web front-end servers.<br>• 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.<br>• 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. |
| | Archiver | DocAve Agent must be installed on at least one of the Web front-end servers. |
| | End-User Archiver | DocAve Agent must be installed on all 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 Welcome 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 |

## Using Hot Key Mode in DocAve Home Page

To access the hot key mode of DocAve Home Page, press the **Ctrl** +**Alt** + **Z** key combination simultaneously on your keyboard while in the DocAve Welcome interface and then press **1** to access the DocAve Home Page.

The following sections provide lists of hot keys for the top level. Each time you want to go back to the top level after accessing the interface of lower level, press **Ctrl** + **Alt** + **Z** on the keyboard.

The following is a list of hot keys for 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 |

| Operation Interface and Hot Key | | | |
|---|---|---|---|
| | | VM Backup & Restore | V |
| Administration | A | Administrator | C |
| | | Content Manager | M |
| | | Deployment Manager | D |
| | | Replicator | R |
| Compliance | C | eDiscovery | E |
| | | Vault | V |
| Report Center | R | Usage Reports | UR |
| | | Infrastructure Reports | I |
| | | Administration Reports | A |
| | | Compliance Reports | C |
| | | DocAve Reports | D |
| | | Usage Pattern Alerting | UP |
| | | Settings | S |
| Storage Optimization | S | Real-time Storage Manager | R |
| | | Scheduled Storage Manager | S |
| | | Connector | C |
| | | Cloud Connect | B |
| | | Archiver | A |
| Control Panel | | P | |
| Job Monitor | | J | |
| Plan Group | | G | |
| Health Analyzer | | H | |
| Log Out | | L | |

## Using Hot Key Mode in Health Analyzer

To access the hot key mode of Health Analyzer, press the **Ctrl** +**Alt** + **Z** key combination simultaneously on your keyboard while in the DocAve Welcome interface. Then press **6** to access Health Analyzer.

The following sections provide lists of hot keys for the top level. Each time you want to go back to the top level after accessing the interface of lower level, press **Ctrl** + **Alt** + **Z** on the keyboard.

The following is a list of hot keys for Health Analyzer.

| Function Name and Hot Key | | | | | | | |
|---|---|---|---|---|---|---|---|
| Profile Manager | P | Create | C | Back | B | | |
| | | | | Next | N | | |
| | | | | Finish | F | Finish | F |
| | | | | | | Finish and Run Now | R |

| Function Name and Hot Key | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Cancel | X | | | | |
| | | View Details | V | Edit | E | Back | B | | |
| | | | | | | Next | N | | |
| | | | | | | Finish | F | Finish | F |
| | | | | | | | | Finish and Run Now | R |
| | | | | | | Cancel | X | | |
| | | | | Cancel | X | | | | |
| | | Edit | E | Back | B | | | | |
| | | | | Next | N | | | | |
| | | | | Finish | F | Finish | F | | |
| | | | | | | Finish and Run Now | R | | |
| | | | | Cancel | X | | | | |
| | | Delete | D | | | | | | |
| | | Run Now | R | | | | | | |
| | | Job Monitor | J | | | | | | |
| | | Close | X | | | | | | |
| Export Report | E | Save | O | | | | | | |
| | | Cancel | X | | | | | | |
| View Details | V | Close | X | | | | | | |
| Stop Scanning | S | | | | | | | | |
| Rescan | RS | | | | | | | | |
| Repair | RP | | | | | | | | |
| Job Monitor | J | | | | | | | | |

# 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.<br>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.<br>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 Migration. To continue using eRoom Migration, close the |
| | eRoom 7.2.2 | |
| | eRoom 7.2.3 | |

| Migration Source | Supported Version | Comment |
|---|---|---|
| | | 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.<br>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.<br>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 | |
| | Livelink 9.6.0 | |
| | Livelink 9.7.0 | |
| | Livelink 9.7.1 | |
| | Windows 2003 32-bit | |

| Migration Source | Supported Version | Comment |
|---|---|---|
| | 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 | Quickr 6.5.1 | |
| | Quickr 7.0.3 | |
| | Quickr 8 | |
| | Quickr 8.5.1 | |

# 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.

#### Required Permissions for the Source

To install and use DocAve File System Migrator properly, ensure the DocAve Agent account in the source is a member of the local **Administrators** group.

#### Required Permissions for the Destination: Migration to 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.
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
        - Managed Metadata Service Administrator with **Full Control** permission
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 the configured Migration Database.
- Member has a Database Role of **db_owner** for the **master** system database.

  ***Note**: This permission is only required when the configured Migration Database does not exist and must be created.

- Member has the Server Role of **dbcreator** to the 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.

## Required Permissions for the Destination: Migration to 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.

**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
- Managed Metadata Service – Term Store Administrator

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

- The user role of SharePoint administrator
- Managed Metadata Service – Term Store Administrator

**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
    - Managed Metadata Service Administrator with **Full Control** permission

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

- **Full Control** to all zones of all Web applications via User Policy for Web Applications.
- Member has a Database Role of **db_owner** for all of the database related to SharePoint, including Content Databases, SharePoint Configuration Database, and Central Admin Database.
- User is a member of the **Site Collection Administrator** group
- Managed Metadata Service
    - Term Store Administrator
    - Managed Metadata Service Administrator with **Full Control** permission

## 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 the 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 the 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 the 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 the 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

3. 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 2007 to 2016 Migration

To install and use SharePoint 2007 to 2016 Migration properly, ensure that the Agent accounts in your SharePoint 2007 and 2016 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 2016 Migration; they are not automatically configured.
   - SharePoint 2007 permissions:
     - User is a member of the Farm **Administrators** group. Since the 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 2016 permissions:
    - User is a member of the Farm **Administrators** group. Since the 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

3. SQL permissions: These permissions must be manually configured prior to using SharePoint 2007 to 2016 Migration; they are not automatically configured.
    - SharePoint 2007 permissions:
        - Database Role of **db_owner** for all the databases related to SharePoint, including Content Databases, Configuration Database, Central Admin Database, and Nintex Workflow Database
    - SharePoint 2016 Permissions:
        - Database Role of **db_owner** for all the databases related to 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 the 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 Administrators work 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 2010 to 2016 Migration

To install and use SharePoint 2010 to 2016 properly, ensure that the Agent account of the SharePoint 2010 and 2016 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 2016 Migration; they are not automatically configured.
    - SharePoint 2010 permissions:
        - User is a member of the Farm **Administrators** group. Since the 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 2016 permissions:
        - User is a member of the Farm **Administrators** group. Since Administrators work 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 2016 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 2016 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 to 2016 Migration

To install and use SharePoint 2013 to 2016 properly, ensure that the Agent account of the SharePoint 2013 and 2016 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.

   ***Note**: Make sure the Agent account of the destination is not the System Account of SharePoint 2016 if SharePoint apps will be migrated by a SharePoint 2013 to 2016 Migration job.

2. SharePoint permissions: These permissions must be manually configured prior to using SharePoint 2013 to 2016 Migration; they are not automatically configured.

   - SharePoint 2013 permissions:
     - User is a member of the Farm **Administrators** group. Since the 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

       ***Note**: Full Control permission is required if SharePoint apps will be migrated by a SharePoint 2013 to 2016 Migration job.

     - User Profile Service Application permissions:
       - 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
   - SharePoint 2016 permissions:
     - User is a member of the Farm **Administrators** group. Since Administrators workacross 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
- Read permission to the **Apps for SharePoint** library in the Catalog Site.

3. SQL permissions: These permissions must be manually configured prior to using SharePoint 2013 to 2016 Migration; they are not automatically configured.

   - SharePoint 2013 permissions:
     - Database Role of **db_owner** for all the databases related with SharePoint, including Content Databases, Configuration Database, Central Admin Database, Nintex Workflow Database, AppService Database, and SettingsService Database
   - SharePoint 2016 permissions:
     - Database Role of **db_owner** for all the databases related with SharePoint, including Content Databases, Configuration Database, Central Admin Database, Nintex Workflow Database, AppService Database, and SettingsService 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 2007/2010/2013 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 2007/2010/2013 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
    - Read permission to the **Apps for SharePoint** library in the Catalog Site.

    ***Note**: To register site collections using the **Scan Mode**, make sure the specified account has the required permission level.

    - When the registered site collections are on-premises site collections, the SharePoint account must have the following permissions:
        - Policy for Web Application: Full Control
        - Database Role of **db_owner** for the Content Databases, SharePoint Configuration Database, and Central Admin Database
    - When the registered site collections are SharePoint Online site collections, make sure the Office 365 account has the **Global Administrator**/SharePoint Administrator role.

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

    ***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.)

    ***Note:** To properly migrate SharePoint 2007/2010/2013 Web parts to SharePoint Online, the user who registers the destination site collection where the migrated Web parts reside must have **Add and Customize Pages** permission to the site collection.

## 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.

### Required Permissions for the Source

Before using DocAve Lotus Notes Migrator, ensure the DocAve Agent account in the source has the following permissions:

1. Local System Permissions: If there are no strict limitations within your organization on the permissions that can be applied, add the source **DocAve Agent Account** to the local **Administrators** group. Otherwise, ensure the source Agent account has the following permissions:
    - Full Control permission to the Lotus Notes installation directory.
    - The permissions listed in Local System Permissions, which are automatically configured by DocAve during installation.
2. Lotus Notes Permission: The permission must be manually configured prior to using DocAve 6 Lotus Notes Migrator; it is not automatically configured.
    - Manager access to all Lotus Notes databases that will be migrated.
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 Migration Database.
    - Member has a Server Role of dbcreator to SQL Server.

### Required Permissions for the Destination: Migration to SharePoint On-Premises

To install and use DocAve Lotus Notes Migrator for SharePoint on-premises properly, ensure that the destination 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.
   - Member has a Server Role of **dbcreator** to SQL Server.

   ***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.

## Required Permissions for the Destination: Migration to 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:

- User is a member of the **Site Collection Administrator** group.
- Managed Metadata Service – Term Store Administrator

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

- The user role of SharePoint administrator
- Managed Metadata Service – Term Store Administrator

**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
    - Full Control
    - Administrator

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

- Full Control permission to all zones of all Web applications via User Policy for Web Applications.
- 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.
- User is a member of the **Site Collection Administrator** group.
- Managed Metadata Service
    - Term Store Administrator
    - Full Control

- Administrator

## 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.

### Required Permissions for the Source

Before using DocAve eRoom Migrator, ensure the DocAve Agent account in the source has the following permissions:

1. Local System Permissions: The permissions listed in Local System Permissions.

   ***Note**: If the source DocAve Agent is not installed on the eRoom file server, the source Agent account must have Read or above permission to the file server directory.

2. eRoom Permission: Full Control to eRoom file server.

### Required Permissions for the Destination: Migration to SharePoint On-Premises

To install and use DocAve eRoom Migrator on the SharePoint on-premises environment properly, ensure that the destination 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 Administrators work 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.

## Required Permissions for the Destination: Migration to SharePoint Online

To install and use eRoom Migrator on the SharePoint Online environment 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:

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

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

- The user role of SharePoint administrator
- Managed Metadata Service – Term Store Administrator

**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
    - Full Control
    - Administrator

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

- Full Control permission to all zones of all Web applications via User Policy for Web Applications.
- 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.
- User is a member of the **Site Collection Administrator** group.
- Managed Metadata Service
    - Term Store Administrator
    - Full Control
    - Administrator

## Livelink Migrator

To install and use DocAve Livelink Migrator properly, ensure that the following permissions are met.

### Required Permissions for the Source

Before using Livelink Migration, ensure that the DocAve Agent account in the source is a member of the local **Administrators** group on the server where the source Livelink Agent is installed.

## Required Permissions for the Destination: Migration to SharePoint On-Premises

Before using Livelink Migration for SharePoint on-premises, ensure that the destination SharePoint 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 Livelink Migrator; they are not automatically configured.
    - User is a member of the **Farm Administrators** group. Since Administrators work 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. 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, Central Admin Database, and DocAve Migration 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.

## Required Permissions for the Destination: Migration to SharePoint Online

Before using Livelink Migration for SharePoint Online, 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:

- User is a member of the **Site Collection Administrator** group.
- Managed Metadata Service – Term Store Administrator

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

- The user role of SharePoint administrator
- Managed Metadata Service – Term Store Administrator

**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
  - Full Control
  - Administrator

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

- **Full Control** to all zones of all Web applications via User Policy for Web Applications.
- 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.
- User is a member of the **Site Collection Administrator** group.
- Managed Metadata Service
  - Term Store Administrator
  - Full Control
  - Administrator

## Exchange Public Folder Migrator

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

### Required Permissions for the Source

To install and use Exchange Public Folder Migration properly, ensure that the DocAve Agent account in the source has the Local System Permissions. 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 Exchange User

To install and use Exchange Public Folder Migration properly, ensure the Exchange user you used when configuring the Exchange public folder connection has the following permissions:

- Full Details
- Folder visible

### Required Permissions for the Destination: Migration to SharePoint On-Premises

To install and use Exchange Public Folder to SharePoint On-Premises Migration properly, ensure that the Agent account has 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:** Since the 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** to SQL server.
    - Member has the Database Role of **db_owner** for the configured Migration Database.
    - Member has the Database Role of **db_owner** for the **master** system database.

***Note**: This permission is only required when the configured Migration Database does not exist and must be created.

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.

## Required Permissions for the Destination: Migration to SharePoint Online

To install and use Exchange Public Folder to SharePoint Online Migration 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:

- User is a member of the **Site Collection Administrator** group
- Managed Metadata Service – Term Store Administrator

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

- The user role of SharePoint administrator
- Managed Metadata Service – Term Store Administrator

**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
    - Managed Metadata Service Administrator with **Full Control** permission

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

- **Full Control** to all zones of all Web applications via User Policy for Web Applications
- Member has a Database Role of **db_owner** for all of the database related to SharePoint, including Content Databases, SharePoint Configuration Database, and Central Admin Database.
- User is a member of the **Site Collection Administrator** group
- Managed Metadata Service
    - Term Store Administrator
    - Managed Metadata Service Administrator with **Full Control** permission

## 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.

### Required Permissions for the Source

Before using DocAve EMC Documentum Migrator, ensure the DocAve Agent account in the source has the following permissions:

1. Local System Permissions: The permissions listed in Local System Permissions.

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

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

2. EMC Documentum Permission: Read permission to EMC Documentum content.

## Required Permissions for the Destination: Migration to SharePoint On-Premises

To install and use DocAve EMC Documentum Migrator on the SharePoint on-premises environment properly, ensure that the destination 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 the 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 the Database Role of **db_owner** in all of the databases related to SharePoint, including Content Databases, SharePoint Configuration Database, and Central Admin Database, and DocAve Migration 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.

## Required Permissions for the Destination: Migration to SharePoint Online

To install and use EMC Documentum Migrator on the SharePoint Online environment 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:

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

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

- The user role of SharePoint administrator
- Managed Metadata Service – Term Store Administrator

**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
    - Full Control
    - Administrator

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

- Full Control permission to all zones of all Web applications via User Policy for Web Applications.
- 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.
- User is a member of the **Site Collection Administrator** group.
- Managed Metadata Service
    - Term Store Administrator
    - Full Control
    - Administrator

## 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.

### Required Permissions for the Source

Before using DocAve Quickr Migrator, ensure the DocAve Agent account in the source has the following permissions:

1. Local System Permissions: If there are no strict limitations within your organization on the permissions that can be applied, add the source **DocAve Agent Account** to the local **Administrators** group. Otherwise, ensure the source Agent account has the following permissions:
    - Full Control permission to the Lotus Notes installation directory.

- Full Control permission to the Quickr installation directory.
- The permissions listed in Local System Permissions, which are automatically configured by DocAve during installation.

2. Quickr Permissions: The permission must be manually configured prior to using DocAve 6 Lotus Notes Migrator; it is not automatically configured.
    - Have the Manager role for all Quickr places that will be migrated.
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 Migration Database.
    - Member has a Server Role of dbcreator to SQL Server.

## Required Permissions for the Destination: Migration to SharePoint On-Premises

To install and use DocAve Quickr Migrator for SharePoint on-premises environments properly, ensure that the destination 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 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.
    - Member has a Server Role of **dbcreator** to SQL Server.

    ***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.

## Required Permissions for the Destination: Migration to 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:

- User is a member of the **Site Collection Administrator** group.
- Managed Metadata Service – Term Store Administrator

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

- The user role of SharePoint administrator
- Managed Metadata Service – Term Store Administrator

**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
    - Full Control
    - Administrator

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

- Full Control permission to all zones of all Web applications via User Policy for Web Applications.
- 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.
- User is a member of the **Site Collection Administrator** group.
- Managed Metadata Service
    - Term Store Administrator
    - Full Control
    - Administrator

## 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 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

# 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 the 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 a network connection or has configured **Agent Proxy Settings** prior to registering the 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

      User has a Database Role of **db_owner** for Content Databases, Config Database, and Central Admin Database.

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

      User has the **Global administrator** or **SharePoint administrator** role

***Note**: To restore SharePoint Online objects, the **Add and Customize Pages** permission is required. You must select **Allow users to run custom script on personal sites** and **Allow users to run custom script on self-service created sites** in **SharePoint admin center** > **Settings** > **Custom Script** to enable the **Add and Customize Pages** permission on the Site Collection Administrator and Global Administrator. Note that the changes will take effect 24 hours after being set.

***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, ensure that the Agent account has the following permissions.

### Agent Account Configured on the SharePoint 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 2010, SharePoint 2013, and SharePoint 2016, the Platform Granular Restore requires the Agent account to have Full Control of all zones of the Web application.

   When restoring the backed up 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
4. 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** and **Security Admin** to SQL Server
- Server Role of dbcreator, Alter any database, or View any definition to the 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 in the Agent group must have the **View Server State** permission to the SQL Server registered in the staging policy, if the **Enable InstaMount for Generating Granular Index** option is selected in the backup plan settings.

***Note**: The Agent account used to back up and restore the SQL Server Report Service must be a member of the local **Administrators** group on the SQL Report Server.

***Note:** To restore the SharePoint apps, make sure the Agent account is not the SharePoint System Account.

## 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 who starts 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) who starts the **SharePoint Server Search 14** service must be added to the **Administrators** group on the corresponding machine. In SharePoint 2013 and SharePoint 2016, the user (logon user) who starts 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 access, launch and activation to the logon user for 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
    - Server 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 Index Server

The Agent account configured on the server where index components reside must be a member of the local **Administrators** group.

## Agent Account Configured on the SQL Server

1. Local System Permissions
    - Backup Operators
    - 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**: Users who can enable the InstaMount must be members of the local **Administrators** group.
2. SQL Server Permissions
    - Database role of **db_owner** for master database.
    - Database role of **db_owner** for all the databases included in the backup plan.

- Server role of **dbcreator** and **processadmin** permission to SQL server.
- Database permission of **Control server** to SQL Server.

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

  The user who restores 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

  ***Note**: To back up and restore the files in File Share directory, the Agent account must have **Read** and **Write** permissions to the File Share directory, and be a member of the local **Administrators** group on the File Share Server.

## 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**.

## Agent Account Configured on Hyper-V hosted VM

1. Local System Permission:
   - Member of the local **Administrators** group
2. Hyper-V VM Permission:
   - Full Control to the folders where the specific VMs are stored
   - Full Control to all of the VMs virtual hard disks

## Agent Account Configured on VMs hosted by ESX/ESXi or vCenter

1. Local System Permissions
   - Member of the local **Administrators** group

## Host Profile Account configured on ESX/ESXi or vCenter Host Server

The account entered in the host profile used to connect ESX/ESXi or vCenter host server must have the **Administrator** role to the ESX/ESXi or vCenter host server.

***Note:** If the user does not have the Administrator role to the ESX/ESXi or vCenter host server, ensure that this user is assigned by a role with at least the privileges in the following table enabled:

| Privileges | | |
|---|---|---|
| Datastore | Allocate space | |
| | Browse datastore | |
| | Low level file operations | |
| | Remove file | |
| Folder | Create folder | |
| Resource | Assign vApp to resource pool | |
| | Assign virtual machine to resource pool | |
| | Create resource pool | |
| vApp | Add virtual machine | |
| | Assign resource pool | |
| | Assign vApp | |
| | Create | |
| Network | Assign network | |
| Virtual machine | Configuration | |
| | Interaction | Answer question |
| | | Configure CD media |
| | | Configure floppy media |
| | | Device connection |
| | | Power On |
| | | Power Off |
| | Inventory | Create new |
| | | Register |
| | | Remove |
| | | Unregister |
| | Snapshot management | Create snapshot |
| | | Remove Snapshot |
| | Provisioning | Allow disk access |
| | | Allow read-only disk access |
| | | Allow virtual machine download |
| | Guest Operations | Guest Operation Modifications |
| | | Guest Operation Program Execute |
| | | Guest Operation Queries |
| Permission | Modify permissions | |
| | Modify role | |
| Alarms | Create Alarm | |
| | Disable alarm action | |
| Host | Inventory | Modify cluster |
| Datastore cluster | Configure a datastore cluster | |
| Global | DisableMethods | |
| | EnableMethods | |
| | License | |

### 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 Manager

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

Agent accounts of DocAve Agent servers that are selected to run restore jobs:

- Local System Permissions
    - Member of the **Administrators** group
- SharePoint Permissions
    - Member of the **Farm Administrators** group

      ***Note:** For both SharePoint 2013 and SharePoint 2016, the SQL Server Data Manager requires the Agent account to have **Full Control** permission to the Web application where the destination node selected in a restore job resides.
- SQL Permissions
    - 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 and the databases configured in the Restore Data from Database jobs

***Note**: To restore apps, the Agent account cannot be a system account.

Agent accounts configured on SQL Servers that are used in staging policies:

- Local System Permissions
  - Member of the **Administrators** group
- SQL Permissions

  ***Note**: If SQL authentication is used in staging policies, make sure the configured accounts have the following permissions.

  - Server Role of **public** for the SQL Server
  - Server Role of **processadmin** in the SQL Server
  - SQL Instance Permission – Control Server
  - Server Role of **dbcreator** in the SQL Server
  - Database Role of **db_owner** for the temporary databases that store the analyzed data
  - Server Role of **sysadmin** in the SQL Server

    ***Note**: This permission is only required when analyzing VHD/VHDX files.

Agent accounts configured on SQL Servers where restoring databases reside:

***Note**: These permissions are required when restoring data from the database.

- Local System Permissions
  - Member of the **Administrators** group
- SQL Permissions
  - Database Role of **db_owner** for the databases configured in the Restore Data from Database jobs
  - Server Role of **public** for the SQL Server

# High Availability

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

## Common Permissions Required for All of the Four Sync Methods

**Agent account configured on the SharePoint servers that are included in the Agent group:**

1. Local System Permissions:

- Member of the **Administrator** local group

2. SharePoint Permissions:
    - Member of Farm Administrators group
    - Full Control permission to the User Profile Service Application
3. SQL Permissions: These permissions must be manually configured prior to using DocAve 6 High Availability.
    - 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 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
    - Server Role of **public** to SQL Server
    - **Control Server** to the destination SQL instance
    - Server role of **securityadmin** to the destination SQL Server

**Agent account configured on the SQL Server:**

1. Local System Permissions:
    - Member of the **Administrators** group
2. 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** to SQL Server

      ***Note**: The Agent account configured on SQL Server must also have the **sysadmin** server role on the standby SQL Server for the following reasons:

        - If you want to perform the High Availability of Standby farm mode for Business Data Connectivity Service, Managed Metadata Service, or Search Service Application, this permission is required so that the Agent account configured on the SharePoint server that is included in the Agent group can be granted the **db_owner** role to the standby databases of those service applications.

- If you want to perform the High Availability of Standby farm mode for a Web application, this permission is required so that the application pool user can be granted the **db_owner** role to the standby database.

**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*.

**VSS Writer account configured on the SQL Server:**

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

**SharePoint 2013/SharePoint 2016 application pool account configured on the SQL Server:**

For SharePoint 2013 and SharePoint 2016, the standby application pool account must exist in the standby SQL Server and have the **db_owner** role to the production database. You can grant the application pool account the server role of **sysadmin** in the standby SQL Server.

**Service application pool account configured on the SharePoint Server:**

If the High Availability group includes the PowerPoint Service Application, the service application pool account configured on the SharePoint server must have the **Write** permission to the *C:\ProgramData\Microsoft\SharePoint* directory in the SharePoint server for storing the temporary file of the Conversion job.

**Agent account configured on the SharePoint Server to start the SP2010StorageOptimizationService.exe process or SP2013StorageOptimizationService.exe process**

If you are about to synchronize the content database with BLOB data and related stub database together to the standby farm with read-only view enabled, make sure the Agent account to start the **SP2010StorageOptimizationService.exe** process or **SP2013StorageOptimizationService.exe** process on the SharePoint server has sufficient permissions in the following scenarios before performing the synchronization job.

- If the Agent account in the standby farm is a different user in the same domain as the Agent account in the production farm, the Agent account in the standby farm must have the **db_owner** role in the production stub database, in order to make sure the standby stub files are readable.
- If the Agent account in the standby farm is in a different domain as the Agent account of the production farm, it is recommended making the domain in the production farm trusted by the domain in the standby farm and granting the Agent account in the standby farm the **db_owner** role in the production stub database. Otherwise, the Agent account in the standby farm must have the **sysadmin** role to the standby SQL instance, in order to make sure the standby stub files are readable.

## Required Permissions for SQL Mirroring Method

Note that * indicates the specific permissions required for SQL Mirroring method.

**Agent account configured on the SharePoint servers that are included in the Agent group:**

1. Local System Permissions:
    - Member of the **Administrator** local group
2. SharePoint Permissions:
    - Member of **Farm Administrators** group
    - Full Control permission to the User Profile Service Application
3. 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 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

- **Control Server** to the destination SQL instance
- Server Role of **public** to SQL Server
- Server role of **securityadmin** to the destination SQL Server. Note that this permission is required for provisioning Managed Metadata Service in the standby farm.
- Server role of **dbcreator** or the **Alter Any Database** permission or **View Any Definition** permission to the SQL Server

**Agent account configured on the SQL Server:**

1. Local System Permissions:
    - Member of the **Administrators** group
2. 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** to SQL Server
    - *Permissions of **Create Endpoint** and **Alter Login** to SQL Server
    - Server Role of **sysadmin** to the destination SQL Server.

**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.** High Availability uses the Agent Temporary Buffer location to store the SQLite database file, which is used for Connector physical device mapping.
- **Read** and **Write** permissions to the directory of *…\AvePoint\DocAve6\Agent\Jobs*.
- ***Read** and **Write** permissions to the sparse file location

  ***Note**: If the spare file location is in File Share, the SQL Server Service account must be a member of the local **Administrators** or **Backup Operators**.

**VSS Writer account configured on the SQL Server:**

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

**SharePoint 2013/SharePoint 2016 application pool account configured on the SQL Server:**

For SharePoint 2013 and SharePoint 2016, the standby application pool account must exist in the standby SQL Server and have the **db_owner** role to the production database. You can also grant the application pool account the server role of **sysadmin** in the standby SQL Server.

**Service application pool account configured on the SharePoint Server:**

If the High Availability group includes the PowerPoint Service Application, the service application pool account configured on the SharePoint server must have the **Write** permission to the *C:\ProgramData\Microsoft\SharePoint* directory in the SharePoint server for storing the temporary file of the Conversion job.

**Agent account configured on the SharePoint Server to start the SP2010StorageOptimizationService.exe process or SP2013StorageOptimizationService.exe process**

If you are about to synchronize the content database with BLOB data and related stub database together to the standby farm with read-only view enabled, make sure the Agent account to start the **SP2010StorageOptimizationService.exe** process or **SP2013StorageOptimizationService.exe** process on the SharePoint server has sufficient permissions in the following scenarios before performing the synchronization job.

- If the Agent account in the standby farm is a different user in the same domain as the Agent account in the production farm, the Agent account in the standby farm must have the **db_owner** role in the production stub database, in order to make sure the standby stub files are readable.
- If the Agent account in the standby farm is in a different domain as the Agent account of the production farm, it is recommended making the domain in the production farm trusted by the domain in the standby farm and granting the Agent account in the standby farm the **db_owner** role in the production stub database. Otherwise, the Agent account in the standby farm must have the **sysadmin** role to the standby SQL instance, in order to make sure the standby stub files are readable.

## Required Permissions for AlwaysOn Availability Group Method

Note that * indicates the specific permissions required for AlwaysOn Availability Group method.

**Agent account configured on the SharePoint servers that are included in the Agent group.**

1. Local System Permissions:
    - Member of the **Administrator** local group
2. SharePoint Permissions:

- Member of **Farm Administrators** group
- Full Control permission to the User Profile Service Application

3. 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 permission of **View server state** to SQL Server
    - Database 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
    - Server Role of **public** to SQL Server
    - **Control Server** to the destination SQL instance
    - Server role of **securityadmin** to the destination SQL Server

      ***Note**: This permission is only required for provisioning Managed Metadata Service in the standby farm.

**Agent account configured on the SQL Server:**

1. Local System Permissions:
    - Member of the **Administrators** group
2. 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
    - Database Role of **dbcreator** and **securityadmin** to SQL Server
    - * Database Permission of **View Server State** to the SQL Server
    - * Database Permission of **Alter Availability Group** to the SQL Server

      ***Note**: The Agent account configured on SQL Server must also have the **sysadmin** server role on the standby SQL Server for the following reasons:

        - If you want to perform the High Availability of Standby farm mode for Business Data Connectivity Service, Managed Metadata Service, or Search Service Application, this permission is required so that the Agent account configured on

the SharePoint server that is included in the Agent group can be granted the **db_owner** role to the standby databases of those service applications.

- If you want to perform the High Availability of Standby farm mode for a Web application, this permission is required so that the application pool user can be granted the **db_owner** role to the standby database.

**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 **Read** and **Write** permissions to the directory of *…\AvePoint\DocAve6\Agent\Jobs*.

High Availability uses the Agent Temporary Buffer location to store the SQLite database file, which is used for Connector physical device mapping.

**VSS Writer account configured on the SQL Server:**

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

**SharePoint 2013/SharePoint 2016 application pool account configured on the SQL Server:**

For SharePoint 2013 and SharePoint 2016, the standby application pool account must exist in the standby SQL Server and have the **db_owner** role to the production database. You can also grant the application pool account the server role of **sysadmin** in the standby SQL Server.

**Service application pool account configured on the SharePoint Server:**

If the High Availability group includes the PowerPoint Service Application, the service application pool account configured on the SharePoint server must have the **Write** permission to the *C:\ProgramData\Microsoft\SharePoint* directory in the SharePoint server for storing the temporary file of the Conversion job.

**Agent account configured on the SharePoint Server to start the SP2010StorageOptimizationService.exe process or SP2013StorageOptimizationService.exe process**

If you are about to synchronize the content database with BLOB data and related stub database together to the standby farm with read-only view enabled, make sure the Agent account to start the **SP2010StorageOptimizationService.exe** process or **SP2013StorageOptimizationService.exe** process on

the SharePoint server has sufficient permissions in the following scenarios before performing the synchronization job.

- If the Agent account in the standby farm is a different user in the same domain as the Agent account in the production farm, the Agent account in the standby farm must have the **db_owner** role in the production stub database, in order to make sure the standby stub files are readable.
- If the Agent account in the standby farm is in a different domain as the Agent account of the production farm, it is recommended making the domain in the production farm trusted by the domain in the standby farm and granting the Agent account in the standby farm the **db_owner** role in the production stub database. Otherwise, the Agent account in the standby farm must have the **sysadmin** role to the standby SQL instance, in order to make sure the standby stub files are readable.

## Required Permissions for Log Shipping Method

Note that * indicates the specific permissions required for Log Shipping method.

***Note**: If you are going to use the Log Shipping method to synchronize the databases in the AlwaysOn Availability group, the required permissions for AlwaysOn Availability Group method must be met as well.

**Agent account configured on SharePoint servers that are included in the Agent group:**

1. Local System Permissions:
    - Member of the **Administrator** group
2. SharePoint Permissions:
    - Member of **Farm Administrators** group
    - Full Control permission to the User Profile Service Application
3. 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
    - Server 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 Server

- Server role of **securityadmin** to the destination SQL Server.

  ***Note**: This permission is only required for provisioning Managed Metadata Service in the standby farm.

**Agent account configured on the SQL Server:**

1. Local System Permissions:
   - Member of the **Administrators** group
2. 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** to SQL Server
   - * **Control Server** to the destination SQL instance

     ***Note**: The Agent account configured on SQL Server must also have the **sysadmin** server role on the standby SQL Server for the following reasons:

     - If you want to perform the High Availability of Standby farm mode for Business Data Connectivity Service, Managed Metadata Service, or Search Service Application, this permission is required so that the Agent account configured on the SharePoint server that is included in the Agent group can be granted the **db_owner** role to the standby databases of those service applications.
     - If you want to perform the High Availability of Standby farm mode for a Web application, this permission is required so that the application pool user can be granted the **db_owner** role to the standby database.

**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**, and **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 **Read** and **Writer** permissions to the database file location (including the path in file share).

**SharePoint 2013/SharePoint 2016 application pool account configured on the SQL Server:**

For SharePoint 2013 and SharePoint 2016, the standby application pool account must exist in the standby SQL Server and have the **db_owner** role to the production database. You can also grant the application pool account the server role of **sysadmin** in the standby SQL Server.

**Service application pool account configured on the SharePoint Server:**

If the High Availability group includes the PowerPoint Service Application, the service application pool account configured on the SharePoint server must have the **Write** permission to the *C:\ProgramData\Microsoft\SharePoint* directory in the SharePoint server for storing the temporary file of the Conversion job.

**Agent account configured on the SharePoint Server to start the SP2010StorageOptimizationService.exe process or SP2013StorageOptimizationService.exe process**

If you are about to synchronize the content database with BLOB data and related stub database together to the standby farm with read-only view enabled, make sure the Agent account to start the **SP2010StorageOptimizationService.exe** process or **SP2013StorageOptimizationService.exe** process on the SharePoint server has sufficient permissions in the following scenarios before performing the synchronization job.

- If the Agent account in the standby farm is a different user in the same domain as the Agent account in the production farm, the Agent account in the standby farm must have the **db_owner** role in the production stub database, in order to make sure the standby stub files are readable.
- If the Agent account in the standby farm is in a different domain as the Agent account of the production farm, it is recommended making the domain in the production farm trusted by the domain in the standby farm and granting the Agent account in the standby farm the **db_owner** role in the production stub database. Otherwise, the Agent account in the standby farm must have the **sysadmin** role to the standby SQL instance, in order to make sure the standby stub files are readable.

## Required Permissions for Platform Backup Log Shipping

Note that * indicates the specific permissions required for Platform Backup Log Shipping method.

**Agent account configured on SharePoint servers that are included in the Agent group.**

1. Local System Permissions:
    - Member of the **Administrator** group
2. SharePoint Permissions:
    - Member of **Farm Administrators** group
    - Full Control permission to the User Profile Service Application
3. 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
    - Server 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
    - **Control Server** to the destination SQL Server
    - Server role of **securityadmin** to the destination SQL Server

      ***Note**: This permission is only required for provisioning Managed Metadata Service in the standby farm.

**Agent account configured on the SQL Server:**

1. Local System Permissions:
    - Member of the **Administrators** group
2. 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** to SQL Server

- *The **Control Server** permission in the destination SQL instance

  ***Note**: The Agent account configured on SQL Server must also have the **sysadmin** server role on the standby SQL Server for the following reasons:

  - If you want to perform the High Availability of Standby farm mode for Business Data Connectivity Service, Managed Metadata Service, or Search Service Application, this permission is required so that the Agent account configured on the SharePoint server that is included in the Agent group can be granted the **db_owner** role to the standby databases of those service applications.
  - If you want to perform the High Availability of Standby farm mode for a Web application, this permission is required so that the application pool user can be granted the **db_owner** role to the standby database.

**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**, and **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 **Read** and **Writer** permissions to the database file location (including the path in file share).

**SharePoint 2013/SharePoint 206 application pool account configured on the SQL Server:**

For SharePoint 2013 and SharePoint 2016, the standby application pool account must exist in the standby SQL Server and have the **db_owner** role to the production database. You can also grant the application pool account the server role of **sysadmin** in the standby SQL Server.

**Service application pool account configured on the SharePoint Server:**

If the High Availability group includes the PowerPoint Service Application, the service application pool account configured on the SharePoint server must have the **Write** permission to the *C:\ProgramData\Microsoft\SharePoint* directory in the SharePoint server for storing the temporary file of the Conversion job.

**Agent account configured on the SharePoint Server to start the SP2010StorageOptimizationService.exe process or SP2013StorageOptimizationService.exe process**

If you are about to synchronize the content database with BLOB data and related stub database together to the standby farm with read-only view enabled, make sure the Agent account to start the **SP2010StorageOptimizationService.exe** process or **SP2013StorageOptimizationService.exe** process on the SharePoint server has sufficient permissions in the following scenarios before performing the synchronization job.

- If the Agent account in the standby farm is a different user in the same domain as the Agent account in the production farm, the Agent account in the standby farm must have the **db_owner** role in the production stub database, in order to make sure the standby stub files are readable.
- If the Agent account in the standby farm is in a different domain as the Agent account of the production farm, it is recommended making the domain in the production farm trusted by the domain in the standby farm and granting the Agent account in the standby farm the **db_owner** role in the production stub database. Otherwise, the Agent account in the standby farm must have the **sysadmin** role to the standby SQL instance, in order to make sure the standby stub files are readable.

## VM Backup and Restore

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

### Required Permissions for Hyper-V VM

To back up and restore the VMs on the Hyper-V host server, ensure the Agent account has the following permissions:

1. Local System Permission
    - A member of the local **Administrators** group
2. Hyper-V VM Permissions
    - Full Control to the folders where the specific VMs are stored
    - Full Control to all of the VMs virtual hard disks

### Required Permissions for ESX/ESXi or vCenter VM

To back up and restore the VMs on the ESX/ESXi or vCenter host server, the Agent account, and the user in the applied host profile must has the following permissions:

1. Local System Permissions for Agent Account
    - A member of the local **Administrators** group
2. ESX/ESXi or vCenter VMs Permissions for the User in the Applied Host Profile
    - Administrator role in the ESX/ESXi or vCenter VMs

***Note:** If the user does not have the Administrator role to the ESX/ESXi or vCenter VMs, ensure that this user is assigned by a role with at least the privileges in the following table enabled:

| **Privileges** | | |
|---|---|---|
| Datastore | Allocate space | |
| | Browse datastore | |
| | Low level file operations | |
| | Remove file | |
| Folder | Create folder | |
| Resource | Assign vApp to resource pool | |
| | Assign virtual machine to resource pool | |
| | Create resource pool | |
| vApp | Add virtual machine | |
| | Assign resource pool | |
| | Assign vApp | |
| | Create | |
| | vApp application configuration | |
| | vApp instance configuration | |
| Network | Assign network | |
| Virtual machine | Configuration | |
| | Interaction | Answer question |
| | | Configure CD media |
| | | Configure floppy media |
| | | Device connection |
| | | Power On |
| | | Power Off |
| | Inventory | Create new |
| | | Register |
| | | Remove |
| | | Unregister |
| | Snapshot management | Create snapshot |
| | | Remove Snapshot |
| | Provisioning | Allow disk access |
| | | Allow read-only disk access |
| | | Allow virtual machine download |
| | Guest Operations | Guest Operation Modifications |
| | | Guest Operation Program Execute |
| | | Guest Operation Queries |
| Permission | Modify permissions | |
| | Modify role | |
| Alarms | Create Alarm | |
| | Disable alarm action | |
| Host | Inventory | Modify cluster |

| Privileges | |
|---|---|
| Datastore cluster | Configure a datastore cluster |
| Global | DisableMethods |
| | EnableMethods |
| | License |

***Note:** If the user does not have the Administrator role to the ESX/ESXi or vCenter VMs, to restore the **Security** settings in the backed up these VMs, except the privileges above-mentioned, this users must have all of the privileges that are enabled to all of the users to be restored.

# 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 the 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.

- Database Role of **db_owner** for FBA database if forms based authentication (FBA) is enabled in SharePoint Web applications.
- 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 the 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

      ***Note:** This permission is required to copy or move My Sites to a destination. However, to ensure a successful copy or move action on My Site, grant the User Profile Service that is associated with the destination Web application **Full Control** and **Administrator with Full Control** permissions to the Application pool account of the destination Web application.
    - User Profile Service Application permission:
        - For SharePoint 2010
            - Use Personal Features
            - Create Personal Site
            - Use Social Features

- For SharePoint 2013 and SharePoint 2016
  - 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

***Note**: To deploy apps, the Agent account cannot be a system account.

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.

     ***Note**: The **db_owner** database role for Nintex Workflow databases is only required in SharePoint 2010 and SharePoint 2013.

   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

The permission requirements for the Agent account used for Content Manager for SharePoint Online are as follows:

- Local System Permissions: 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 SharePoint On-Premises Site Collections

The user that is used to register the 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
- Managed Metadata Service: Term Store Administrator
- The **Read** permission to the **Apps for SharePoint** library in the App Catalog Site Collection

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

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

### 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:

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

- User is a member of the **Site Collection Administrator** group.
- 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

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

***Note**: To copy or move SharePoint Online objects, the **Add and Customize Pages** permission is required. Users with the role of SharePoint administrator or Site Collection Administrator have the **Add and Customize Pages** permission, but you must select **Allow users to run custom script on personal sites** and **Allow users to run custom script on self-service created sites** in **SharePoint admin center** > **Settings** > **Custom Script** to enable the **Add and Customize Pages** permission to these users. Note that the changes will take effect 24 hours after being set.

## Deployment Manager

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

### Deployment Manager for SharePoint On-Premises

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 the 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/SharePoint 2016:
        - 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/SharePoint 2016
            - 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

***Note**: To deploy the newsfeed, the Agent account must be a system account. To deploy apps, the Agent account cannot be a system account.

### 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

## Deployment Manager for SharePoint Online

The following permissions are required for Deployment Manager to perform a Deployment Manager job for SharePoint Online.

### Local System Permissions for Agent Account

The Agent account is on the machine that has network connection or has **Agent Proxy Settings.** This must be done before registering the SharePoint Online site collections.

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 perform the Deployment Manager job for SharePoint Online must have the following permissions:

- User is a member of the **Site Collection Administrator** group.
- User Profile Service Application:
  - Follow People and Edit Profiles
  - Use Tags and Notes
- Managed Metadata Service: Term Store Administrator
- Apps: Read permission to the library "Apps for SharePoint" in Catalog Site.

***Note**: To deploy SharePoint Online objects, the Add and Customize Pages permission is required. You must select **Allow users to run custom script on personal sites** and **Allow users to run custom script on self-service created sites** in **SharePoint admin center** > **settings** > **Custom Script** to enable the Add and Customize Pages permission on the Site Collection Administrator and Global Administrator. Note that the changes will take effect 24 hours after being set.

## 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 the 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
       - User Profile Connection Permission: Full Control
       - Use Personal Features

        - Create Personal Site
        - Use Social Features
    - For SharePoint 2013 and SharePoint 2016
        - User Profile Connection Permission: Full Control
        - 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

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 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
- 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
  - 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:
    - User Profile Connection Permission: Full Control
    - User Profile Administrator
    - 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

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

- Full Control permission to all zones of all Web applications via User Policy for Web Applications.
- 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.
- User Profile Service Application:
    - User Profile Connection Permission: Full Control
    - User Profile Administrator
    - 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

**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.
- Permission for User Profile:
  - 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

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

- The user role of SharePoint administrator
- Managed Metadata Service: Term Store Administrator
- Permissions for User Profile Service

- Create Personal Site (required for personal storage, newsfeed, and followed content)
- Follow People and Edit Profile
- Use Tags and Notes

***Note**: To replicate SharePoint Online objects, the **Add and Customize Pages** permission is required. Users with the role of SharePoint administrator or Site Collection Administrator have the **Add and Customize Pages** permission, but you must select **Allow users to run custom script on personal sites** and **Allow users to run custom script on self-service created sites** in **SharePoint admin center** > **settings** > **Custom Script** to enable the **Add and Customize Pages** permission to these users. Note that the changes will take effect 24 hours after being set.

# 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 the 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

To install and use Report Center properly, ensure that the Agent account has the following permissions.

***Note**: For a SharePoint Online environment, the user used to register this site collection must be a member of the **Site Collection Administrators** group. If the site collections are added through **Scan Mode**, the user adding the site collections must be a member of **Global Administrators**. Additionally, to report on the site collection quotas via the Configuration Report, the site collection user must be a **Global Administrator** as well.

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 the 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
        - User Profile Service Application Administrator
        - Use Personal Features (For SharePoint 2010 only)
        - Create Personal Site
        - Use Social Features (For SharePoint 2010 only)
        - Follow People and Edit Profile (For SharePoint 2013 only)
        - Use Tags and Notes (For SharePoint 2013 only)
    - 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 Content Database and Stub Database

      ***Note**: To use the Search Usage report and Referrers report, the Agent account must have the **db_owner** role for SharePoint 2010 Web Analytics Service Databases

      To use the Search Usage report for SharePoint 2013, the Agent account must have the **db_owner** role for the SharePoint 2013 Search Service Application Analytics Reporting databases and Search Service Application Administration databases.

      To use the SharePoint Search Service report, the Agent account must have the **db_owner** for the SharePoint 2010 or SharePoint 2013 WSS_Logging Database

      To use the Configuration Reports, the Agent account must have the **db_owner** role for the SharePoint 2010 or SharePoint 2013 User Profile Service Application Databases

      To use the Best Practice Reports, the Agent account must have the **db_owner** role for the SharePoint 2010 or SharePoint 2013 Metadata Service Application Databases
4. Registered SharePoint Sites Permission:

- The site collection user used to register the site collection must be a member of Site Collection Administrators.

  ***Note**: If you want to use Configuration Reports or Storage Trends report to report on the site collection quota, the site collection user must be a member of SharePoint Administrators group.

- The following permissions are required, if using **Scan Mode** to add the registered site collections:
  - To scan the SharePoint Online site collections or OneDrive for Business libraries, the user must be a member of:
    - SharePoint Administrators
    - Local Administrators
  - To scan the SharePoint on-premises site collections, the user must have:
    - Full Control to all zones of all Web applications via the User Policy for Web Applications
    - Database Role of **db_owner** for all the databases related with SharePoint, including Content databases, Config 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, 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 the 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.
    - Database role of **securityadmin** since SharePoint API is required the permission to enable RBS.

### 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 the 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 the database role of **db_owner** for all the DocAve stub databases.
   - Member has a Server Role of **dbcreator** in SQL Server since it must create a stub database before performing any Connector job.

     ***Note**: The **dbcreator** role is only required for Windows Authentication.
   - Member has the server role of **securityadmin** in SQL Server for enabling RBS.

## 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 | |
| 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 Folder/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 Folders/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 Subfolders 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 a 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:

***Note**: If the Web application pool account is not the Agent account, the Web application pool account must have the **Read** permission to the ***…\DocAve6\Agent*** folder.

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 Web front-end servers)
- Full Control to GAC in order to install BLOB Provider .dll files into GAC)
- Full Control to **Microsoft SQL Remote Blob Storage** Folder to reconfigure maintainer configuration file

## Cloud Connect

Refer to the section below for the required permissions for installing and using DocAve Cloud Connect.

### Agent Account Permissions

To install and use Cloud Connect 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 Cloud Connect; they are not automatically configured.
    - User is a member of the **Farm Administrators** group. Since the 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 Cloud Connect; 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 the database role of **db_owner** for all the DocAve stub databases.
- Member has a Server Role of **dbcreator** in SQL Server since it must create a stub database before performing any Cloud Connect job.

  ***Note**: The **dbcreator** role is only required for Windows Authentication.
- Member has the server role of **securityadmin** in SQL Server for enabling RBS.

### Local System Permissions

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

***Note**: If the Web application pool account is not the Agent account, the Web application pool account must have the **Read** permission to the ***…\DocAve6\Agent*** folder.

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 Web front-end servers)
- Full Control to GAC in order to install BLOB Provider .dll files into GAC)
- Full Control to **Microsoft SQL Remote Blob Storage** Folder to reconfigure maintainer configuration file

## Archiver

To install and use Archiver properly, ensure that the Agent account has the following permissions.

### SharePoint 2010, 2013, and 2016

To install and use Archiver for SharePoint 2010, 2013, and 2016 nodes properly, ensure 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
   - User Profile Service Application permissions for SharePoint 2013 and 2016:
     - 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
   - Managed Metadata Service:
     - Term Store Administrator
     - Member of the **Administrators** group with 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

  ***Note**: If you choose to use Windows Authentication when configuring the Archiver Database, make sure the Agent account has this permission. If you choose to use SQL Authentication, make sure the user specified has this permission.

## SharePoint Online

To install and use Archiver for SharePoint Online nodes properly, ensure the Agent account and site collection users (specified when registering site collection) have the following permissions:

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 the required permissions.
   - SQL Permissions: User has the database role of **db_owner** for the Archiver Database.
   - When site collections are registered using the **Scan Mode**, the Agent account must be a member of the local **Administrators** group.
2. Site collection user permissions:
   - The **Global administrator** role
   - Managed Metadata Service: Term Store Administrator
   - User Profile Service: User Profile Service Administrator

   ***Note**: When site collections are registered using the **Scan Mode**, make sure the Office 365 account has the **SharePoint administrator** role.

   ***Note**: To run incremental jobs on SharePoint Online personal sites or self-service created sites, make sure the SharePoint admin center setting **Custom Script** is enabled.

## 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

# Appendix E: User-defined Certificates

Refer to the following information to use a user-defined certificate for communication between the DocAve Manager and DocAve Agent. This instruction uses the Windows Server 2008 R2 Operating System as an example.

## Generating a Certificate

If you do not have a user-defined certificate that meet the requirements, AvePoint provides a method to generate a certificate. Complete the following steps to generate a certificate:

### Adding the Certificates Snap-in to Microsoft Management Console

Complete the steps below to add the Certificates Snap-in to the Microsoft Management Console.

1. On the machine where you are about to install the DocAve Manager, navigate to **Start** > **Run**. The **Run** pop-up window appears.
2. In the **Open** text box, type **MMC** to open the Microsoft Management Console.
3. In the Microsoft Management Console window, click the **File** menu and select **Add/Remove Snap-in …** from the drop-down list.

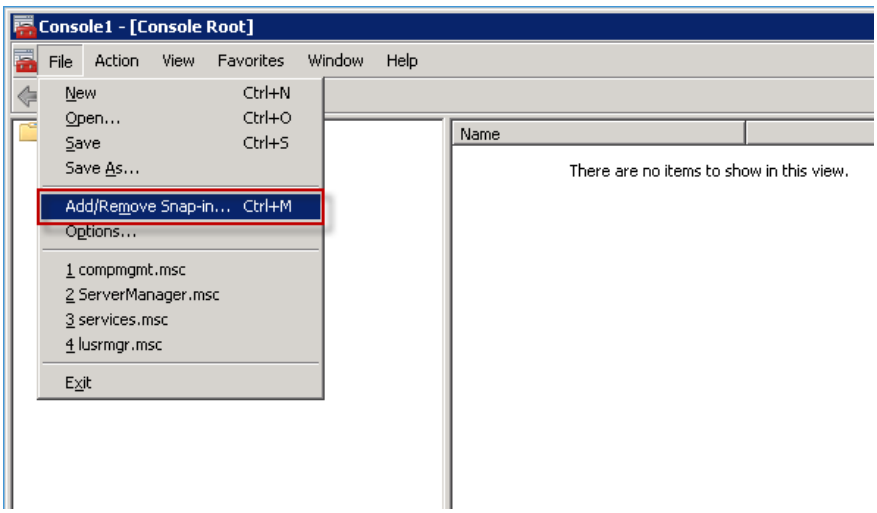



**Figure 9: Clicking Add/Remove Snap-in… from the drop-down list.**

4. The **Add or Remove Snap-ins** dialog box appears. Select **Certificates** and click **Add**.

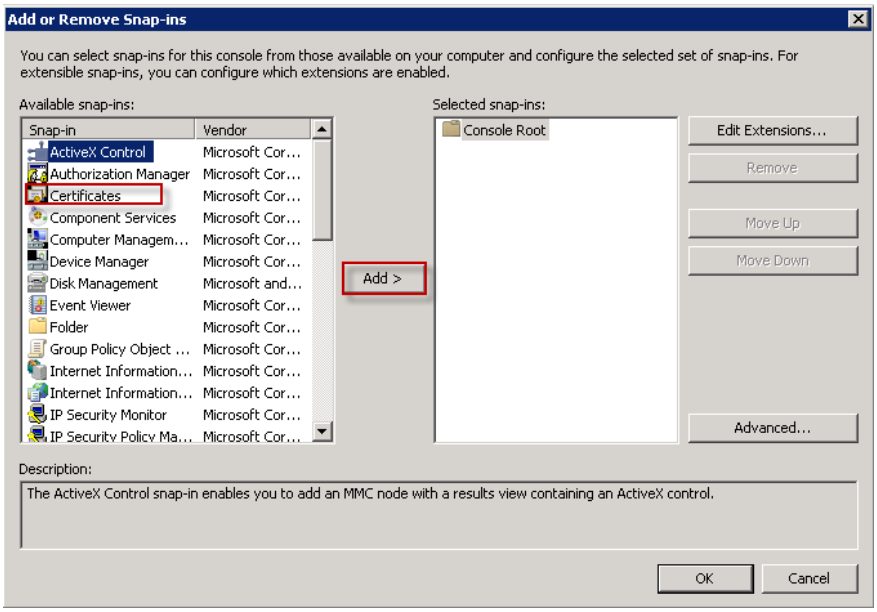



**Figure 10: Selecting Certificates and clicking Add.**

5. The **Certificates snap-in** dialog box appears. Select the **Computer account** option, then click **Next**.

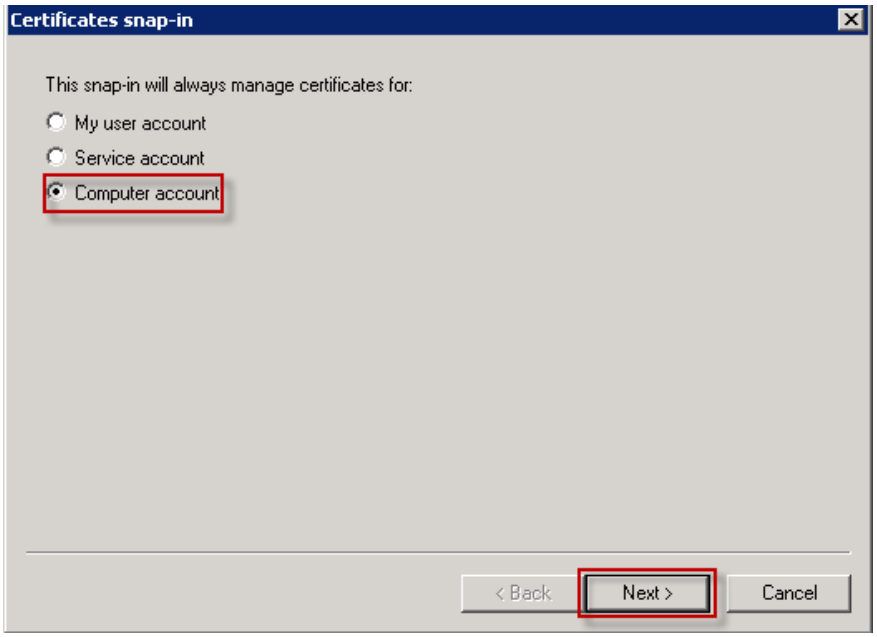



**Figure 11: Selecting the Computer account option and clicking Next.**

6. In the **Select Computer** dialog box, click **Finish**.
7. In the **Add or Remove Snap-ins** dialog box, click **OK** to close it.

## Creating a Request File

1. In the **Console Root** window, navigate to **Certificates (Local Computer)** > **Personal** and right-click **Certificates**.
2. From the drop-down list, navigate to **All Tasks** > **Advanced Operations** > **Create Custom Request**.

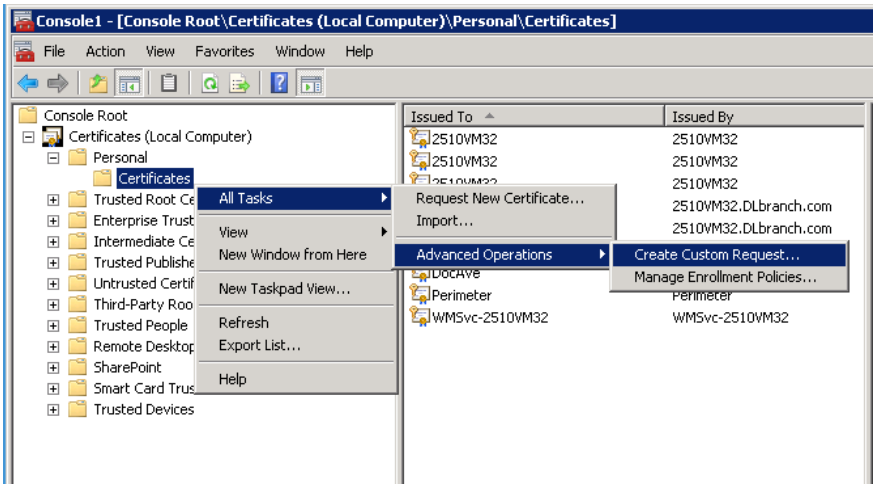



**Figure 12: Navigating to All Tasks > Advanced Operations > Create Custom Request.**

3. The **Certificate Enrollment** wizard appears. Click **Next** until the **Custom request** interface appears.
4. From the drop-down list of **Template**, select **Subordinate Certification Authority**. Click **Next**.

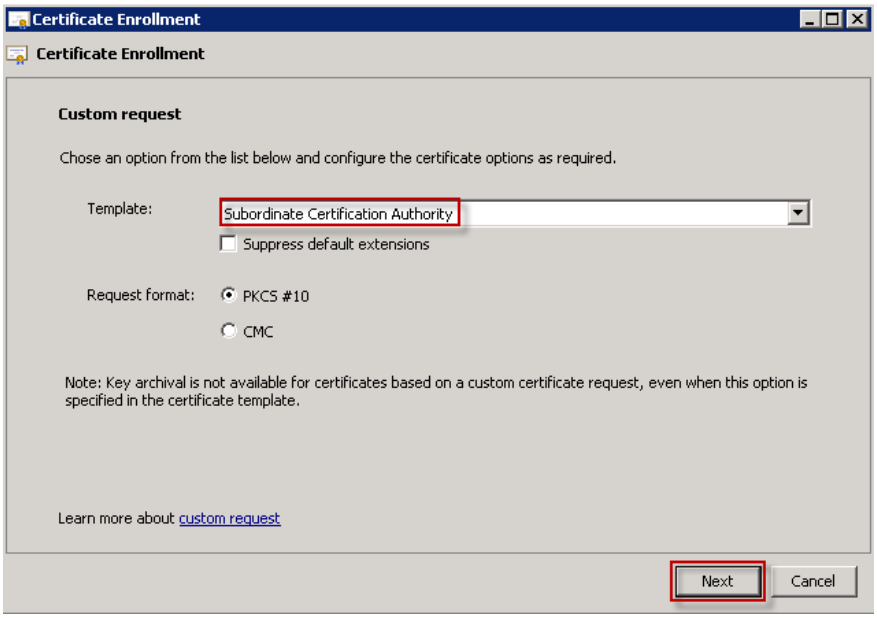



**Figure 13: Selecting Subordinate Certification Authority.**

5. The **Certificate Information** interface appears. Click **Details**, and then click **Properties**.

6. The **Certificate Properties** window appears. From the drop-down list of **Type**, select a type of the subject, and enter the value in the text box of **Value**. Click **Add**.

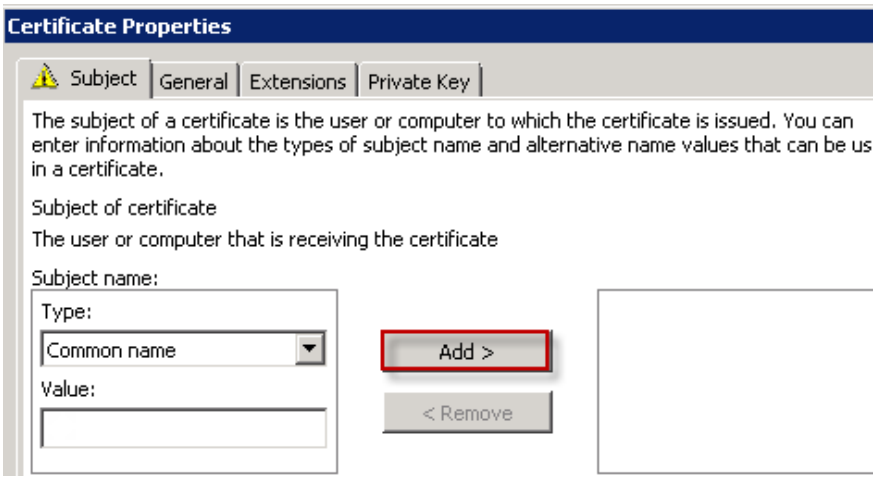



**Figure 14: Selecting Common name and enter the value.**

7. Select the **Extensions** tab, and click the **Extended Key Usage (application policies)**.
8. From the **Available options**, select **Server Authentication**, and click **Add** to add it to the **Selected options**.

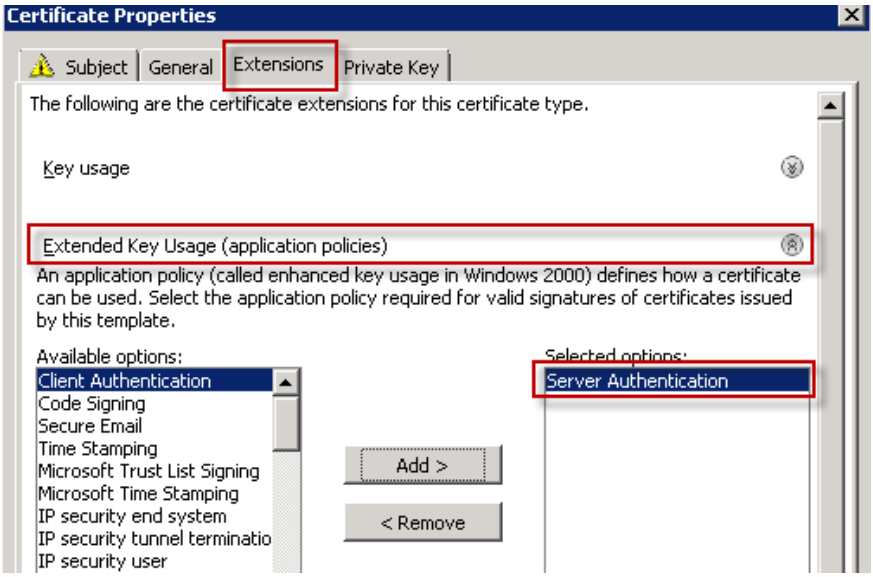



**Figure 15: Selecting Server Authentication.**

***Note**: You can also select **All application policies**, because it includes the **Server Authentication**.

9. Select the **Private Key** tab, and click the **Key options**. Make sure that the **Make private key exportable** checkbox is selected.

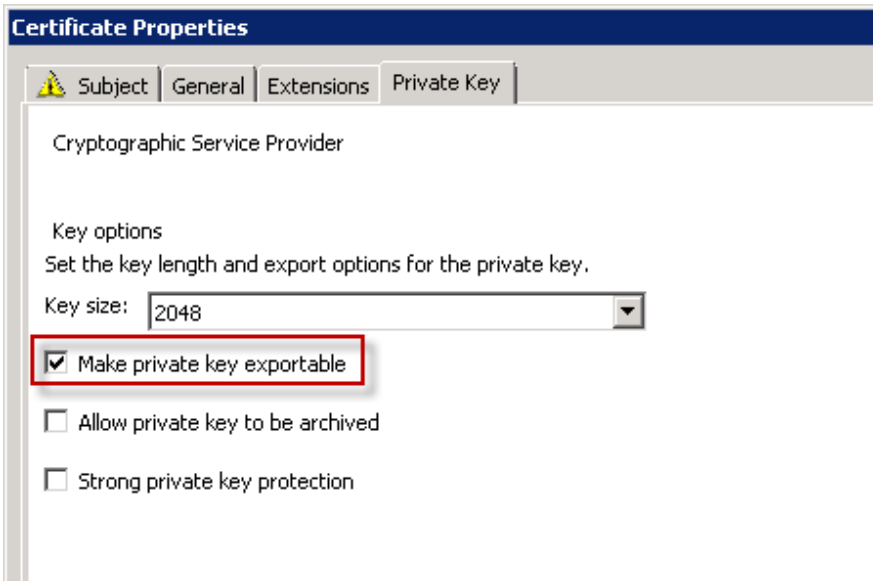



**Figure 16: Checking the checkbox of Make private key exportable.**

10. Click the **Key type**, and select **Exchange** option.

    ***Note**: The product does not support certificates whose key types are **Signature**.

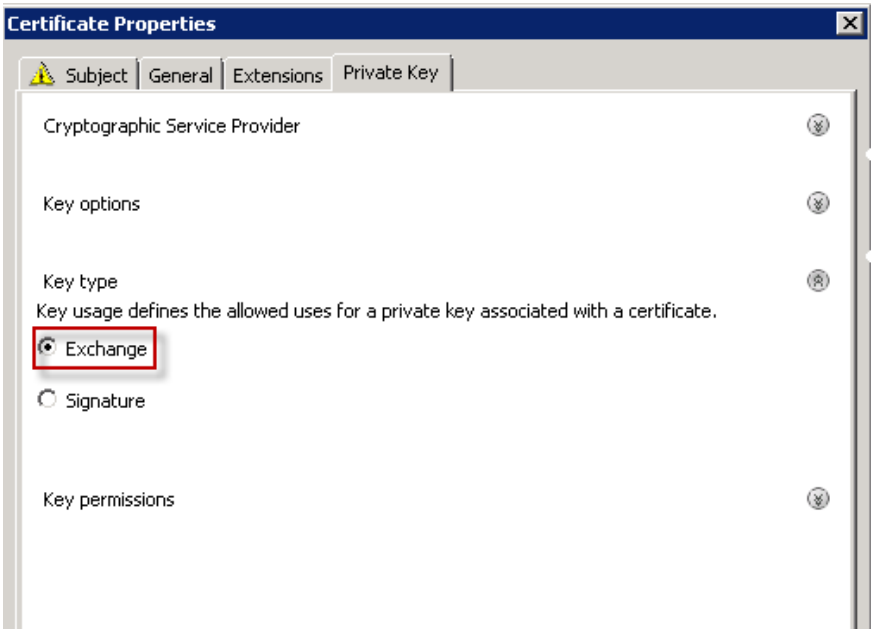



**Figure 17: Selecting Exchange as the Key Type.**

11. Click **OK** or **Apply**, and the **Certificate Properties** window disappears.

12. Click **Next** in the **Certificate Information** interface.
13. Enter the location and name of your certificate request, and then click **Finish**. The request file will be generated under the entered path.

## Requesting and Downloading a Certificate

Complete the following steps to request and download a certificate.

1. Access the Certificate Authority of the Domain, and select **Request a certificate**.

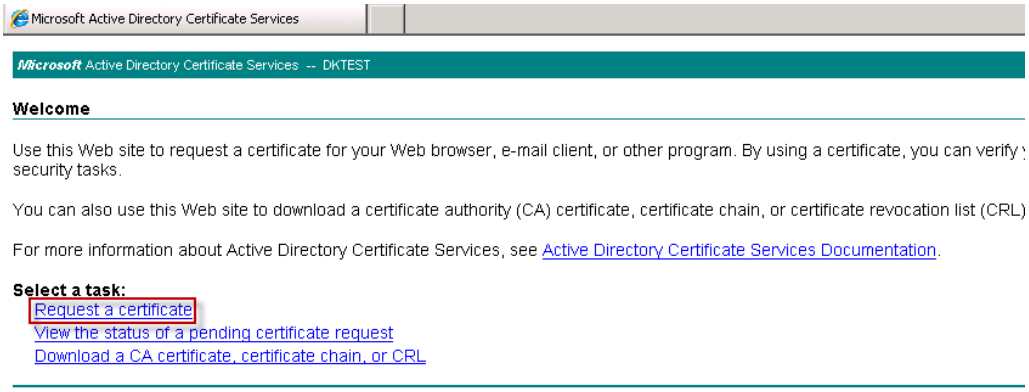



**Figure 18: Selecting Request a certificate.**

2. Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file** option.

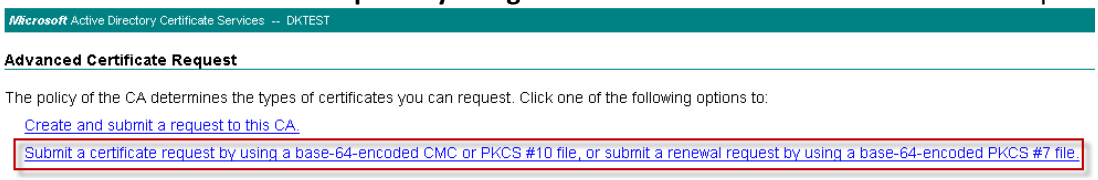



**Figure 19: Selecting Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file option.**

3. Find the request file that is generated in step 20, and open it with notepad. Copy the content to the **Saved Request** text box. Select **Certificate Template**. The selected template must be the same as that of the requested certificate. Click **Submit**.

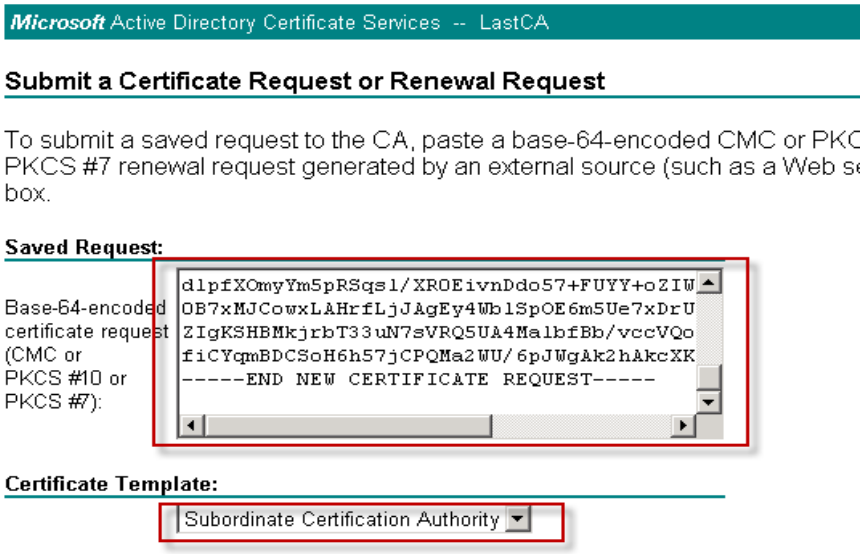



**Figure 20: Pasting the Saved Request and selecting Certificate Template.**

4. Download the certificate to your local machine and save it.

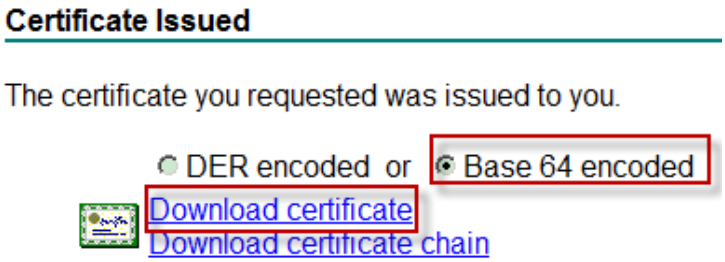



**Figure 21: Downloading the certificate.**

# Importing a Certificate

If your local machine has the certificate, complete the following steps to import the certificate to the Microsoft Management Console.

1. Add the Certificates Snap-in to Microsoft Management Console, and refer to Adding the Certificates Snap-in to Microsoft Management Console for more details.
2. In the **Console Root** window, navigate to **Certificates (Local Computer)** > **Personal** and right-click **Certificates**.
3. From the drop-down list, navigate to **All Tasks** > **Import…**.

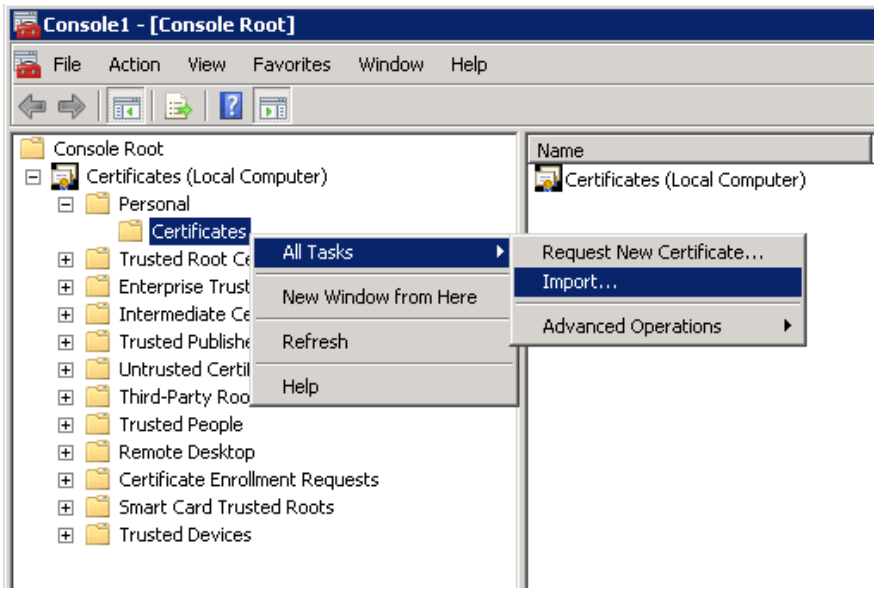



**Figure 22: Navigating to All Tasks > Import… and clicking Import….**

4. The **Certificate Import Wizard** appears. Select **Local Machine** option, and click **Next**.
5. In the **File to Import** interface, **Browse** the certificate file in the **.PFX** format. Click **Next**.
6. In the **Private key protection** interface, type the **Password**. Select the **Mark this key as exportable** check box.
7. Click **Finish** to close the wizard.

## Exporting a Certificate

Complete the steps below to export the certificate from Microsoft Management Console.

1. Add the Certificates Snap-in to Microsoft Management Console, and refer to Adding the Certificates Snap-in to Microsoft Management Console for more details.
2. In the **Console Root** window, navigate to **Certificates (Local Computer)** > **Personal** > **Certificates**.
3. Right-click the certificate.
4. Navigate to **All Tasks** > **Export…** and click it. The **Certificate Export Wizard** appears.

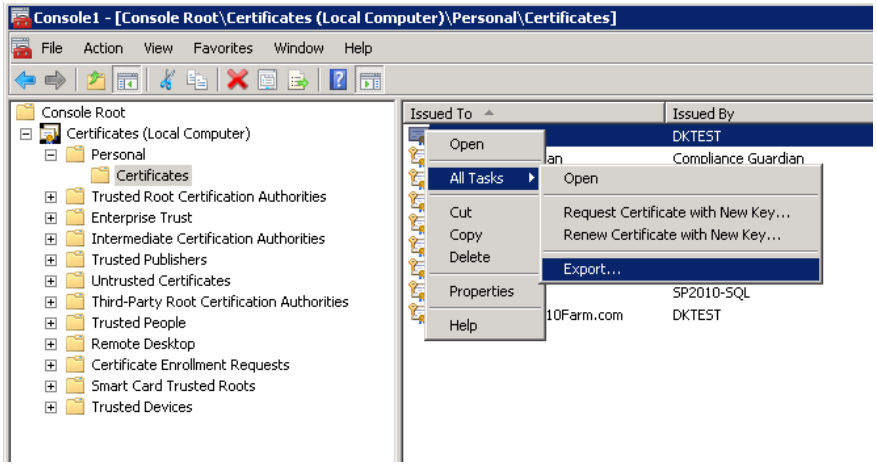



**Figure 23: Navigating to All Tasks > Export… and clicking Export….**

5. Click **Next**.
6. In the **Export Private Key** interface, select **Yes, export the private key** option and click **Next**.
7. In the **Export File Format** interface, select the options according to your situation and click **Next**.
8. Configure the security to protect the private key. Click **Next**.
9. Enter the name of the certificate you want to export. Click **Next**.
10. Click **Finish** to close the wizard.

# Checking Key Type Using Script

AvePoint provides a script for checking the Key Type of a certificate. Follow the instructions below to use the script.

1. Start Notepad.
2. Type the command below in the Notepad window.

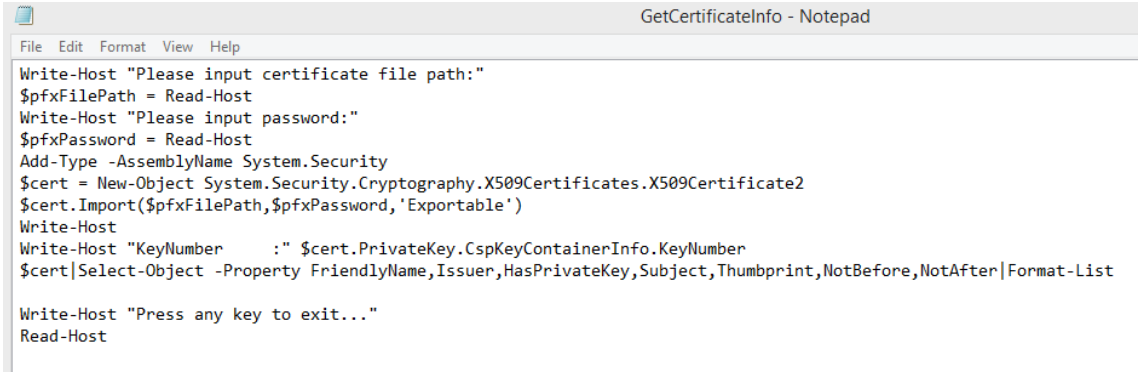



**Figure 24: Typing the command in the Notepad window.**

3. Save the command in a file with **.ps1** file name extension.

4. Right-click the file and select **Run with PowerShell**.
5. Input the full path of the certificate file, then press **Enter**.
6. Input the password, then press **Enter**.
7. The Key Type will display in the **KeyNumber**.

# Appendix F: 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 extracted Manager installation package, and double click **SetupManager.exe** to run it. Complete the following steps:

1. From the welcome screen, click **Next**.
2. Choose to create a new answer file or modify an existing answer file for the DocAve Agent.
    - **Create a new answer file for DocAve 6 Manager** – Select this option to create a new Answer file for the 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 or click **Browse** to browse for an answer file.

      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 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 collections and managements, monitor SharePoint activities and return the data to the Control service for processing. 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 available, causing the installation to fail.

    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 available, causing the installation to be failed.

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

11. For the report service database, you can select **Use the previous database settings** or configure it yourself. 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 **Use the previous database settings** or configure it yourself. 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**: The DocAve Auditor database should be created on a SQL server that does not stores the SharePoint databases. Since DocAve Auditor Controller retrieves data from the SharePoint content 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.

o **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.

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

1. Click **Start** on the server that contains the extracted Manager installation package, and open the Windows PowerShell by right-clicking on it and selecting **Run as administrator**.
2. Enter the following command, and press **Enter** to import the **UnattendedInstallation.dll** file:

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

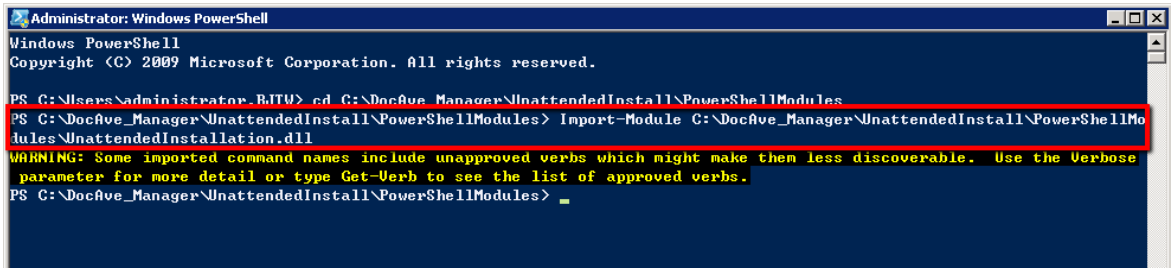



**Figure 25: Importing the UnattendedInstallation.dll file.**

***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. The

warnings have no effect on importing the file. 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 extracted Manager installation package.
2. Right click on the **UnattendedInstallationLauncher.bat** file, and select **Run as administrator** to run it.

   ***Note**: If the script is not loaded successfully while running the **UnattendedInstallationLauncher.bat** file, use the `Get-ExecutionPolicy` command in Windows PowerShell to get the value of the execution policy. If the value is not to **AllSigned**, **Unrestricted**, or **RemoteSigned**, use the `Set-ExecutionPolicy` command to set the value as **AllSigned**, **Unrestricted**, or **RemoteSigned**, and run the **UnattendedInstallationLauncher.bat** file again.

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 performing the DocAve Manager installation, 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.<br><br>The permissions of the user specified here are as follows:<br>• If the specified user is the local administrator of the destination machine, it can be used directly. Enter .*administrator* for the *Username* parameter.<br>• 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.<br><br>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.<br><br>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 extracted DocAve Manager installation package.<br><br>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.<br><br>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.<br><br>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 environment checking logs 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:\Folder\Log.txt.*<br><br>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.<br><br>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.<br><br>***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.<br><br>***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.<br><br>The permissions of the user specified here are as follows:<br>• If the specified user is the local administrator of the destination machine, it can be used directly. Enter .*administrator* for the *Username* parameter.<br>• 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.<br><br>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.<br><br>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 extracted DocAve Manager installation package (Manager ZIP file). The format of the path is: *C:\package*.<br><br>Quote the path if it contains any special character or space. |
| -AnswerFilePath | Required | The local path where you saved the Answer file.<br><br>The path must be detailed to the name of the Answer file. For example, *C:\AnswerFile.xml*. |

| Parameter | Type | Description |
|---|---|---|
| -RemoteTempPath | Required | A local path on the destination machine that the DocAve Manager is installed to. The format of the path is: *C:\temp*.<br>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.<br><br>The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Folder\Log.txt.*<br><br>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.<br><br>***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.<br><br>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. |

| Parameter | Type | Description |
|---|---|---|
| -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.<br><br>***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 Manager installed. The format of the username is: domain\username.<br><br>The permissions of the user specified here are as follows:<br>• If the specified user is the local administrator of the destination machine, it can be used directly. Enter *.\administrator* for the *Username* parameter.<br>• 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.<br><br>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. |
| -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.<br><br>The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Folder\Log.txt.*<br><br>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.<br><br>The path specified in this parameter must be detailed to the name of the log file. For example, *C:\ManagerConfigInfor.xml.*<br><br>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.<br><br>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.<br><br>***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 | Type | Description |
|---|---|---|
| | | 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" -UseControlFailoverDatabase 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.<br><br>***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.<br><br>The permissions of the user specified here are as follows:<br>• If the specified user is the local administrator of the destination machine, it can be used |

| Parameter | Type | Description |
|---|---|---|
| | | directly. Enter .*administrator* for the *Username* parameter.<br>• 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.<br>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.<br><br>Quote the password if it contains any special character or space. |
| -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.<br>***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.<br>***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. |

| Parameter | Type | Description |
|---|---|---|
| | | ***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.<br>***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.<br>***Note**: If **–ControlDatabaseServer** or **–ControlDatabaseName** is used, **-ControlPassphrase** must be configured. |
| -UseControlFailoverDatabase | Optional | Enable the failover database server function for the Control database.<br><br>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.<br>***Note**: If the parameter **–UseControlFailoverDatabase** is used, -**ControlFailoverDatabase** must be configured. |
| -UseWindowsAuthenticationFor ControlDatabase | Optional | Using this parameter to change the authentication of the Control database between Windows Authentication and SQL Authentication.<br><br>If the current authentication being used in the destination Control 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 database on the destination machine.<br>***Note**: If the parameter **–UseWindowsAuthenticationForControlDatabase** is used, **-ControlDatabaseUsername** must be configured. |
| -ControlDatabasePassword | Optional | The password of the user specified above.<br>***Note**: If the parameter **–UseWindowsAuthenticationForControlDatabase** is |

| Parameter | Type | Description |
|---|---|---|
| | | used, **-ControlDatabasePassword** must be configured.<br>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. |
| -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.<br>***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.<br>***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.<br><br>If the Report database on the destination machine is not associating a failover database server, set the |

| Parameter | Type | Description |
|---|---|---|
| | | 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.<br>***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.<br><br>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. |
| -ReportDatabaseUsername | Optional | The new account you want to use to authenticate the Report database on the destination machine.<br>***Note**: If the parameter **–UseWindowsAuthenticationForReportDatabase** is used, the **–ReportDatabaseUsername** must be configured. |
| -ReportDatabasePassword | Optional | The password of the user specified above.<br>***Note**: If the parameter **–UseWindowsAuthenticationForReportDatabase** is used, the **–ReportDatabasePassword** must be configured.<br>Quote the password if it contains any special character or space. |
| -AuditorDatabaseServer | Optional | The new server you want to use for the Auditor database.<br>***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.<br>***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.<br><br>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. |

| Parameter | Type | Description |
|---|---|---|
| | | *__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.<br><br>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.<br>*__Note__: If the parameter __–UseWindowsAuthenticationForAuditorDatabase__ is used, the __–AuditorDatabaseUsername__ must be configured. |
| -AuditorDatabasePassword | Optional | The password of the user specified above.<br>*__Note__: If the parameter __–UseWindowsAuthenticationForAuditorDatabase__ is used, the __–AuditorDatabasePassword__ must be configured.<br>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.<br><br>The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Folder\Log.txt.*<br><br>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.<br><br>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 |

| Parameter | Type | Description |
|---|---|---|
| | | entered in **TargetName** parameter, this parameter must be entered.<br><br>***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. |

## 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" -UseControlFailoverDatabase 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.<br><br>***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 you want to install the DocAve Manager. The format of the username is: domain\username.<br><br>The permissions of the user specified here are as follows:<br>• If the specified user is the local administrator of the destination machine, it can be used directly. Enter *.\administrator* for the *Username* parameter.<br>• 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.<br><br>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.<br><br>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.<br>***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. |

| Parameter | Type | Description |
|---|---|---|
| | | ***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.<br>***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.<br>***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.<br>***Note**: If **–ControlDatabaseServer** or **–ControlDatabaseName** is used, **-ControlPassphrase** must be configured. |
| -UseControlFailoverDatabase | Optional | Set *True* as the value of this parameter and verify whether you can specify a failover SQL Server for the Control database. |
| -ControlFailoverDatabase | 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. |
| -UseWindowsAuthentication ForControlDatabase | 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.<br><br>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. |

| Parameter | Type | Description |
|---|---|---|
| -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.<br>***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 verify as the Report database.<br>***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. |
| -UseWindowsAuthentication ForReportDatabase | 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.<br><br>Quote the password if it contains any special character or space. |
| -AuditorDatabaseServer | Optional | The new server you want to verify for the Auditor database.<br>***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.<br>***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. |
| -UseWindowsAuthentication ForAuditorDatabase | Optional | Set *True* or *False* as the value of this parameter and verify whether you can use Windows Authentication for the Auditor database. |

| Parameter | Type | Description |
|---|---|---|
| -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.<br><br>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.<br><br>The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Folder\Log.txt.*<br><br>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.<br><br>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.<br><br>***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 |

| Parameter | Type | Description |
|---|---|---|
| | | 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 retrieves 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
```

# Appendix G: Unattended Installation of DocAve Agent

The DocAve Agent can be installed remotely using the unattended installation after the Manager 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 extracted Manager installation package, and double click *SetupManager.exe* to run it. You will be guided through the following steps.

1. From the welcome screen, click **Next**.
2. Choose to create a new answer file or modify an existing answer file for the DocAve Agent.
    - **Create a new answer file for DocAve 6 Agent** – Select this option to create a new Answer file for the 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.
3. Click **Next**.
4. Carefully review the DocAve License Agreement.
5. 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**.
6. 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.
7. 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**.

8. 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**.

9. 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**.

10. Set up the Agent configuration:
    - **Manager Passphrase** – Enter the Manager Passphrase of the Manager where the Agent is being registered. If you don't know 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.
    - **DocAve Agent Account** – Specify the username and password of the Agent account under which the Agent activities are performed. Refer to Installing DocAve Agents for the detailed permissions required for this account.
11. Click **Next** to access the **Installation Summary** page.
12. 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.

# Importing 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.

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`

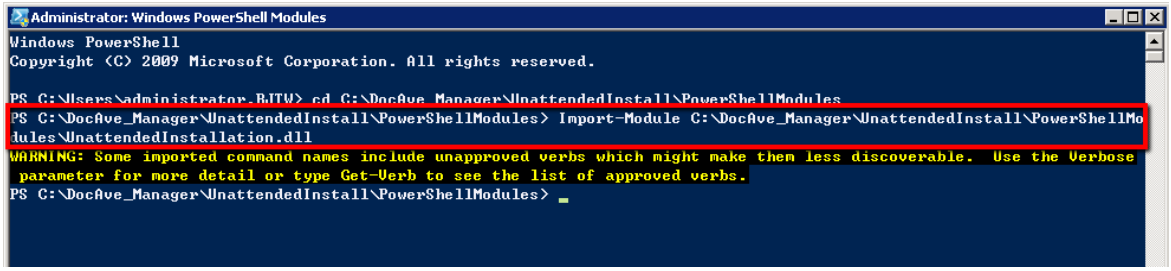



**Figure 26: Importing the UnattendedInstallation.dll file.**

***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. The warning has no effect on importing files. 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 extracted Manager installation package.
2. Right-click the **UnattendedInstallationLauncher.bat** file, and select **Run as administrator** to run it.

   ***Note**: If the script is not loaded successfully while running the **UnattendedInstallationLauncher.bat** file, use the `Get-ExecutionPolicy` command in the Windows PowerShell to get the value of the execution policy. If the value is not **AllSigned**, **Unrestricted**, or **RemoteSigned**, use the `Set-ExecutionPolicy` command to set the value as **AllSigned**, **Unrestricted**, or **RemoteSigned**, and run the **UnattendedInstallationLauncher.bat** file again.

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.<br><br>***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.<br><br>The permissions of the user specified here are as follows:<br>• If the specified user is the local administrator of the destination machine, it can be used directly. Enter *.\administrator* for the *Username* parameter.<br>• 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.<br><br>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.<br><br>Quote the password if it contains any special character or space. |

| Parameter | Type | Description |
|---|---|---|
| -CheckEnvironmentFilePath | Required | The local path of the DocAve.dat file that is residing in the extracted DocAve Agent installation package.<br><br>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.<br><br>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.<br><br>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.<br><br>The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Folder\Log.txt.*<br><br>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.<br><br>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.<br><br>***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 |

| Parameter | Type | Description |
|---|---|---|
| | | 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.<br><br>***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.<br><br>The permissions of the user specified here are as follows: |

| Parameter | Type | Description |
|---|---|---|
| | | • If the specified user is the local administrator of the destination machine, it can be used directly. Enter .*administrator* for the *Username* parameter.<br>• 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.<br>• 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.<br><br>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 extracted DocAve Agent installation package (Agent ZIP file). The format of the path is: C:\package.<br><br>Quote the path if it contains any special character or space. |
| -AnswerFilePath | Required | The local path where you saved the Answer file.<br><br>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.<br><br>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.<br><br>The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Folder\Log.txt.*<br><br>If the specified log file does not exist, it will be generated automatically. |

| Parameter | Type | Description |
|---|---|---|
| -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.<br><br>***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.<br><br>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. |

## Installing DocAve Agent in Parallel Command

The unattended installation process of DocAve Agent supports installing Agents in parallel. Each `Start-job` command must include the command of installing one Agent. For example:

1. Enter the follow commands:

```
Start-Job -ScriptBlock {Import-Module
C:\DocAve_Manager\UnattendedInstall\PowerShellModules\UnattendedInstallation.dll;

Install- DAAgent -TargetName hostmachine -Username AvePoint\DocAve -Password Ave -
PackageFilesFolder C:\DocAve_Agent -AnswerFilePath C:\AnswerFile1.xml

-RemoteTempPath C:\TempFolder -ProductType DocAve}
```

2. Press **Enter** after entering a `Start-job` command to install one DocAve Agent. All of the `Start-job` commands will be executed in parallel to install the DocAve Agents across all of the specified servers.

To view the reports of executing the `Start-job` commands, enter the `Get-job` command, and then press **Enter**.

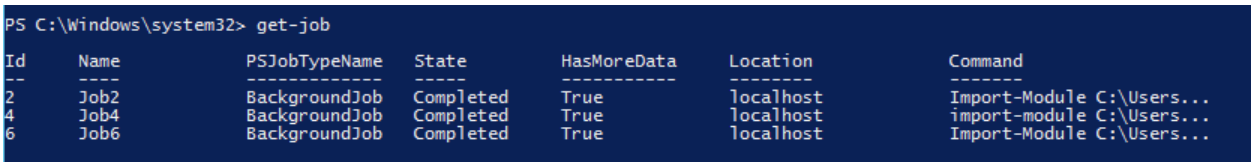



**Figure 27: Entering the `Get-job` command to view the reports.**

To view details on processing one `Start-job` command for one Agent installation job, enter the `Receive-Job -ID Job ID -Keep` command, and then press **Enter**. The `Job ID` refers to the ID of the job that you want to check.

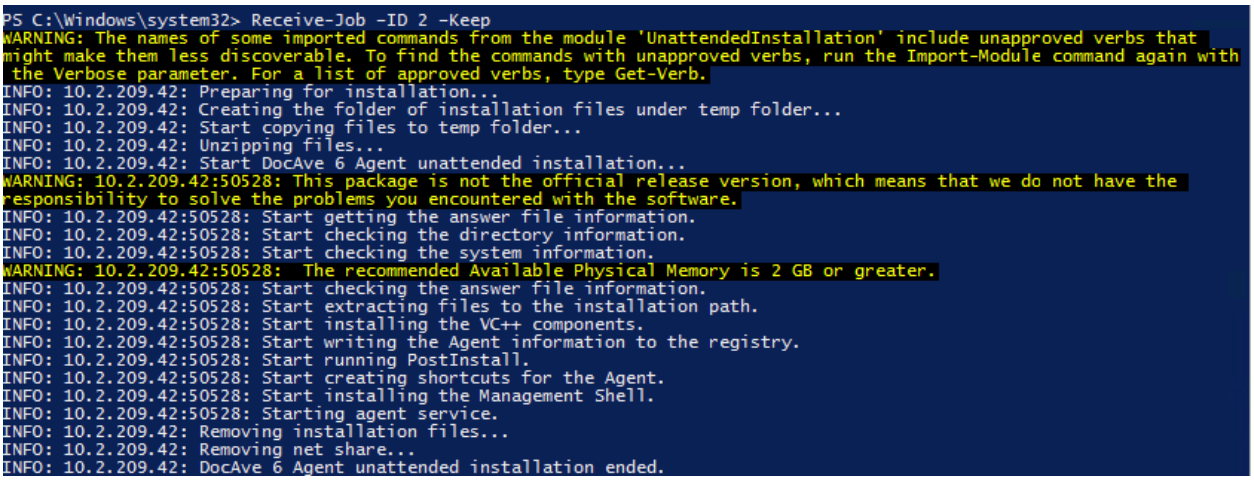



**Figure 28: Getting details on one Agent installation job.**

***Note**: If the machine that executes the `Install- DAAgent` command and the server where the Agent will be installed both use the **Internet Protocol Version 6 (TCP/IPv6)**, you must enter the `-UseIPv6forCommunication` parameter after the `Install- DAAgent` command.

## 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.<br><br>***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.<br><br>The permissions of the user specified here are as follows:<br>• If the specified user is the local administrator of the destination machine, it can be used directly. Enter .*administrator* for the *Username* parameter.<br>• 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.<br><br>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.<br><br>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.<br><br>The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Folder\Log.txt.*<br><br>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. |

| Parameter | Type | Description |
|---|---|---|
| | | The content format of the generated .xml file is the same as the Agent Answer File.<br><br>The path specified in this parameter must be detailed to the name of the log file. For example, *C:\ManagerConfigInfor.xml.*<br><br>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.<br><br>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.<br><br>***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.<br><br>***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.<br><br>The permissions of the user specified here are as follows:<br>• If the specified user is the local administrator of the destination machine, it can be used directly. Enter *.\administrator* for the *Username* parameter.<br>• 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.<br><br>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.<br><br>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. |

| Parameter | Type | Description |
|---|---|---|
| -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. |
| -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.<br><br>The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Folder\Log.txt*.<br><br>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.<br><br>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.<br><br>***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 |

| Parameter | Type | Description |
|---|---|---|
| | | 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 if the configuration information you want to use for DocAve Agent is valid or not. You can verify the configuration information for the Agents installed remotely through the use of Unattended Installation, and you can modify the configuration information for the Agents installed locally through the use of installation wizard.

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.<br><br>***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.<br><br>The permissions of the user specified here are as follows:<br>• 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.<br><br>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.<br><br>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.<br><br>The path specified in this parameter must be detailed to the name of the log file. For example, *C:\Folder\Log.txt.*<br><br>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.<br><br>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 |

| Parameter | Type | Description |
|---|---|---|
| | | IPv6 address is entered in **TargetName** parameter, this parameter must be entered.<br><br>***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
```

# Appendix H: Unattended Uninstallation of DocAve Manager

DocAve Manager can be uninstalled remotely using the unattended uninstallation. Prior to uninstalling DocAve Manager, please ensure the Manager services being removed are not in use by another process.

The following sections offer detailed instruction on the unattended uninstallation of DocAve Manager.

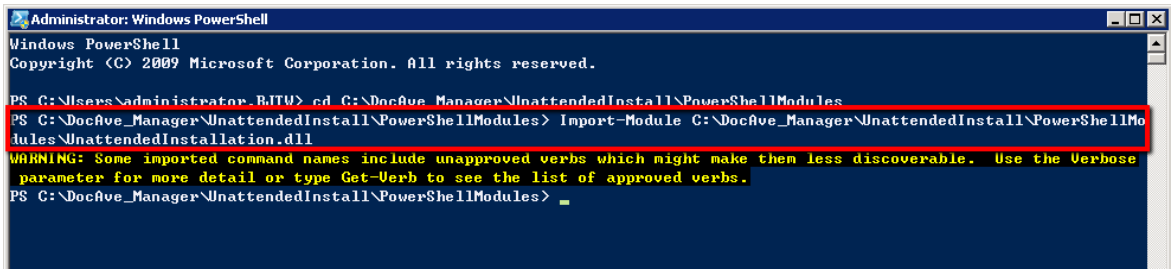
## Importing the UnattendedInstallation.dll File

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

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 the **UnattendedInstallationLauncher.bat** file, and select **Run as administrator** to run it.

   ***Note**: If the script is not loaded successfully while running the **UnattendedInstallationLauncher.bat** file, use the `Get- ExecutionPolicy` command in the Windows PowerShell to get the value of the execution policy. If the value is not **AllSigned**, **Unrestricted**, or **RemoteSigned**, use the `Set-ExecutionPolicy` command to set the value as

**AllSigned**, **Unrestricted**, or **RemoteSigned**, and run the **UnattendedInstallationLauncher.bat** file again.

Now that you have imported the **UnattendedInstallation.dll** file, you can use the command in the following section to uninstall the DocAve Manager.

# Command and Command Parameters for DocAve Manager Unattended Uninstallation

The command for uninstalling DocAve Manager remotely is **Uninstall-DAManager**. For example:

```
Uninstall-DAManager -TargetName hostmachine -Username AvePoint\DocAve -Password "Ave"
-RemoteTempPath "C:\TempFolder" -ProductType "DocAve" -RemoveConfigurationFile "true"
-RemoveBuiltinDB "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 you want to uninstall the DocAve Manager.<br><br>***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 uninstall the DocAve Manager. The format of the username is: domain\username.<br><br>The permissions of the user specified here are as follows:<br>• If the specified user is the local administrator of the destination machine, it can be used directly. Enter .*administrator* for the *Username* parameter.<br>• 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.<br><br>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. |
| -RemoteTempPath | Required | A local path on the destination machine from where you want to uninstall the DocAve Manager. The format of the path is: *C:\temp*.<br>The path will be used to store the temporary files generated during the DocAve Manager unattended uninstallation. The temporary files will be deleted as soon as the unattended uninstallation finishes. |
| -ProductType | Required | This parameter is used to identify the product you are uninstalling from other AvePoint's products.<br><br>Enter **DocAve** as the value of this parameter when you uninstall DocAve products. |
| -RemoveConfigurationFile | Optional | This parameter is used to select whether to remove all the folders and the configuration files generated by DocAve Manager installation. |
| -RemoveBuiltinDB | Optional | This parameter is used to select whether to remove the built-in databases created during the DocAve Manager installation. |

# Appendix I: Unattended Uninstallation of DocAve Agent

DocAve Agent can be uninstalled remotely using the unattended installation.

The following sections offer detailed instruction on the unattended uninstallation of DocAve Agent.

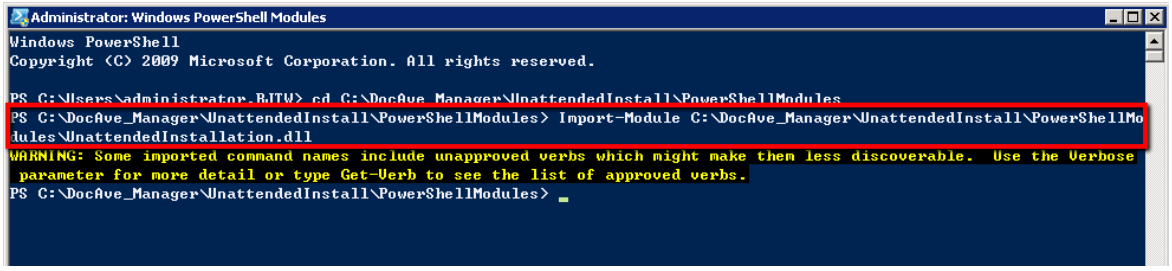
## Importing the UnattendedInstallation.dll File

Before performing the DocAve Agent unattended uninstallation, the **UnattendedInstallation.dll** file must be imported into Windows PowerShell 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 the **UnattendedInstallationLauncher.bat** file, and select **Run as administrator** to run it.

***Note**: If the script is not loaded successfully while running the **UnattendedInstallationLauncher.bat** file, use the `Get- ExecutionPolicy` command in the Windows PowerShell to get the value of the execution policy. If the value is not **AllSigned**, **Unrestricted**, or **RemoteSigned**, use the `Set-ExecutionPolicy` command to set the value as **AllSigned**, **Unrestricted**, or **RemoteSigned**, and run the **UnattendedInstallationLauncher.bat** file again.

Now that you have imported the **UnattendedInstallation.dll** file, you can use the command in the following section to uninstall the DocAve Agent.

# Command and Command Parameters for DocAve Agent Unattended Uninstallation

The command for uninstalling DocAve Agent remotely is `Uninstall-DAAgent`. For example:

```
Uninstall-DAAgent -TargetName hostmachine -Username AvePoint\DocAve -Password "Ave" -RemoteTempPath "C:\TempFolder" -ProductType "DocAve"-RemoveConfigurationFile "true" -DisableEBSORRBSsettings  "true"
```

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 uninstall the DocAve Agent.<br><br>***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 uninstall the DocAve Agent. The format of the username is: domain\username.<br><br>The permissions of the user specified here are as follows:<br>• If the specified user is the local administrator of the destination machine, it can be used directly. Enter .*administrator* for the *Username* parameter.<br>• 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.<br>• 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.<br><br>Quote the password if it contains any special character or space. |
| -RemoteTempPath | Required | A local path on the destination machine from where you want to uninstall the DocAve Agent. The format of the path is: C:\temp. |

| Parameter | Type | Description |
|---|---|---|
| | | The path will be used to store the temporary files generated during the DocAve Agent unattended uninstallation. The temporary files will be deleted as soon as the unattended uninstallation finishes. |
| -ProductType | Required | This parameter is used to identify the product you are uninstalling from other AvePoint's products.<br><br>Enter *DocAve* as the value of this parameter when you uninstall DocAve products. |
| -RemoveConfigurationFile | Optional | This parameter is used to select whether to remove all the folders and the configuration files generated by DocAve Agent installation. |
| -DisableEBSORRBSsettings | Optional | This parameter is used to select whether to disable the EBS/RBS settings in the corresponding SharePoint farm. If the EBS/RBS settings are disabled, the Storage Optimization stubs cannot be accessed. Set the value to **false** if you want to reinstall the DocAve 6 Agent on the same machine later. |

# 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 and international copyright laws and no part of this publication may be reproduced, modified, displayed, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of AvePoint, 3 Second Street, Jersey City, NJ 07311, USA or, in the case of materials in this publication owned by third parties, without such third party's consent. Notwithstanding the foregoing, to the extent any AvePoint material in this publication is reproduced or modified in any way (including derivative works and transformative works), by you or on your behalf, then such reproduced or modified materials shall be automatically assigned to AvePoint without any further act and you agree on behalf of yourself and your successors, assigns, heirs, beneficiaries, and executors, to promptly do all things and sign all documents to confirm the transfer of such reproduced or modified materials to AvePoint.

**Trademarks**
AvePoint®, DocAve®, the AvePoint logo, and the AvePoint Pyramid logo are registered trademarks of AvePoint, Inc. with the United States Patent and Trademark Office. These registered trademarks, along with all other trademarks of AvePoint used in this publication are the exclusive property of AvePoint and may not be used without prior written consent.

Microsoft, MS-DOS, Internet Explorer, Office, Office 365, SharePoint, Windows PowerShell, SQL Server, Outlook, Windows Server, Active Directory, and Dynamics CRM 2013 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe Acrobat and Acrobat Reader are trademarks of Adobe Systems, Inc.

All other trademarks contained in this publication are the property of their respective owners and may not be used without such party's consent.

**Changes**
The material in this publication is for information purposes only and is subject to change without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, AvePoint makes no representation or warranty, expressed or implied, as to its completeness, accuracy, or suitability, and assumes no liability resulting from errors or omissions in this publication or from the use of the information contained herein. AvePoint reserves the right to make changes in the Graphical User Interface of the AvePoint software without reservation and without notification to its users.

AvePoint, Inc.
Harborside Financial Center, Plaza 10
3 Second Street, 9th Floor
Jersey City, New Jersey 07311
USA