



Content Productivity Suite

Pre-requisites and Installation Guide

CPS Version: 9.0

7 August 2026

Status: Published

Table of Contents

1. INTRODUCTION	4
1.1. MIGRATION ACCELERATOR DEPLOYMENT OVERVIEW	4
1.2. INSIGHTS AND MONITOR DEPLOYMENT OVERVIEW	5
2. SYSTEM REQUIREMENTS	7
2.1. APPLICATION SERVER(S)	7
2.1.1. MIGRATION ACCELERATOR HARDWARE REQUIREMENTS	7
2.1.2. INSIGHTS AND MONITOR HARDWARE REQUIREMENTS	8
2.1.3. SOFTWARE REQUIREMENTS	9
2.1.4. SOURCE SPECIFIC LICENSING REQUIREMENTS	9
2.1.5. NETWORK AND SECURITY	10
2.1.5.1. PORTS AND ENDPOINT REQUIREMENT	10
2.1.5.2. ANTI-VIRUS SOFTWARE	12
2.1.5.3. FIREWALL WHITELIST	12
2.2. CPS SQL DATABASE REQUIREMENTS	14
2.2.1. SQL HARDWARE REQUIREMENTS	14
2.2.2. SOFTWARE REQUIREMENTS	15
2.3. CORE ACCOUNT REQUIREMENTS	16
2.3.1. SOURCE SPECIFIC USER ACCOUNT REQUIREMENTS	17
3. SHAREPOINT GRAPH DISCOVERY PREREQUISITES	21
3.1. CREATE AN APP REGISTRATION IN AZURE PORTAL	21
3.2. ADD PERMISSIONS TO THE APPLICATION	21
3.2.1. GRAPH API PERMISSIONS	21
3.2.2. REST API PERMISSIONS	21
3.3. GENERATE CERTIFICATE	21
4. GOOGLE WORKSPACE PREREQUISITES	23
5. STAGING DATABASE BEST PRACTICES AND GUIDELINES	24
6. INSTALLATION	26
6.1. WELCOME SCREEN	26
6.2. PRE-REQUISITE CHECKS	26
6.3. DATABASE INFORMATION	27
6.4. CHOOSE ITEMS TO INSTALL	28
6.5. CONFIRM AND COMPLETE INSTALLATION	28

6.6. TROUBLESHOOTING INSTALLATION PROBLEMS	30
6.7. SHAREPOINT ONLINE GRAPH DISCOVERY TOOL SETUP	30
7. LAUNCH APPLICATION	31
8. UPGRADE/UNINSTALL THE SOFTWARE	32
8.1. UPGRADE PROCESS	32
8.2. UNINSTALL SOFTWARE	32
8.3. INSTALLING UPGRADED SOFTWARE	32
8.4. SHAREPOINT ONLINE GRAPH DISCOVERY TOOL SETUP	33

About this Guide

This document contains detailed instructions on how to install Content Productivity Suite.

For additional information or assistance see our knowledge base at

<https://support.proventeq.com>

Audience

This guide is designed for product users, operators, and supervisors who are familiar with the migration project and its associated environment.

1. INTRODUCTION

Content Productivity Suite provides a suite of applications to migrate and analyse content management systems.

Within the suite there are separately licenced products: -

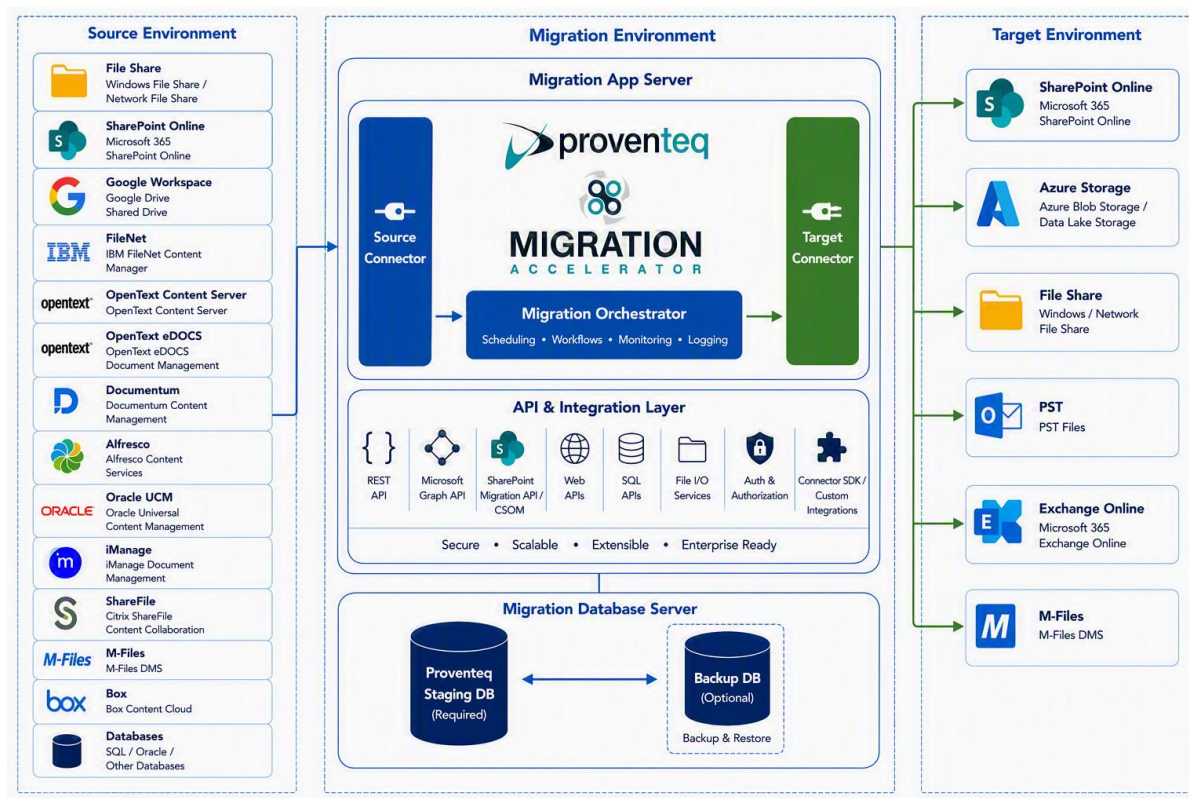
Proventeq Migration Accelerator is a versatile enterprise grade migration engine that is deployed as a Windows .NET application. It allows you to configure different source and target system connections in the migration engine, perform content analysis, set up advanced content transformation rules, execute and monitor an end-to-end migration.

Proventeq Orchestrator is a content management automation product. It has the ability to automate end to end migration activities. It provides a user interface and API end points to create and schedule migration jobs.

Proventeq Insights is a content management analysis product. It supports all the same source systems as Migration Accelerator and has the ability to create reports with details of item duplication, embedded links and highlight any incompatibility issues if the data is migrated to SharePoint.

Proventeq Monitor is a content monitoring product. It supports all the same source systems as Migration Accelerator and has the ability to analyse and create reports having details of source content permissions oversharing.

1.1. Migration Accelerator Deployment Overview



The diagram highlights the source, migration and target environment. The actual architecture will depend upon the source platform being migrated and migration options.

- **Migration App Server** - The application server(s) work in conjunction with an SQL database server (termed the staging database)
- The **SQL server** will host the migration staging database, which will be used to store migration configuration along with source system data discovery and processing details. It does NOT store actual item content.
- The target environment will be SharePoint Online/OneDrive or SharePoint On Premise.

Rest API/File IO For some sources, CPS uses the relevant source system API to capture and retrieve information, for others it captures the information by direct access to the underlying content management file and database storage (which affects Firewall port configuration).

DB Backup - For FileNet, eDocs/Hummingbird, Meridio, it's recommended that the Source database associated with the Content Management System is copied and then CPS is configured to access this snapshot rather than the 'Live' database.

For iManage it's mandatory that a backup copy is copied into the same SQL server that hosts the CPS Staging database.

SharePoint CSOM/Migration API – Items are migrating to SharePoint Online using the Migration API or using CSOM API for SharePoint On-Premise.

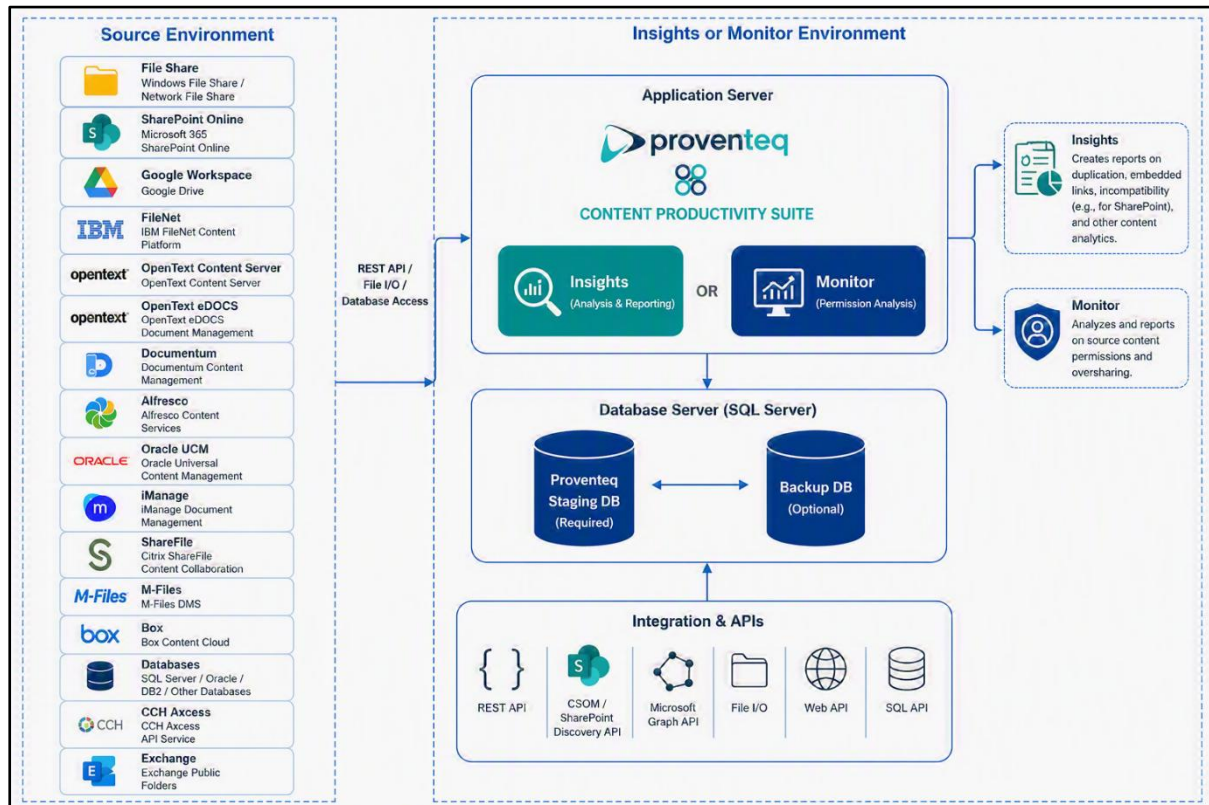
NOTE: Supported SQL Platforms

For FileNet, Meridio and Oracle UCM; Microsoft SQL, IBM DB2 and Oracle are supported source system database platforms.

1.2. Insights and Monitor Deployment Overview

Proventeq Insights and Monitor are separate products, that provides standalone discovery and analysis capabilities. It is not required as part of a migration solution using Migration Accelerator as this contains it's own discovery and analysis capabilities.

If a solution requires Migration Accelerator, Insights and Monitor, it's possible for these to share the same App server but CPS allows only one active background job at any one time so it's not possible to be running Insights, Monitor discovery and a migration concurrently.



The deployment diagram highlights the source environment and Insights or Monitor environment.

- The Insights or Monitor environment includes an application server and an SQL database server (termed the staging database), which should be configured within the customer network.
- The application server with Content Productivity Suite application installed and configured. The database server will host the Staging database, which will be used to store configuration information along with information captured from the source for analysis. It does NOT store item content.

2. SYSTEM REQUIREMENTS

The Content Productivity Suite (CPS) is an application which requires an application server (Windows server) and an SQL database (hosted by Microsoft SQL Server). The servers can be provisioned on-premises or in the cloud.

The system requirements fall into the following components: -

- Hardware and software requirements for the CPS server
- Network and Security requirements (Ports, Anti-Virus, Whitelists)
- CPS database server requirements
- Core account permissions
- Source specific account permissions

It's essential that all the steps are carried out to ensure a successful installation and operation of the CPS product.

Software License

The CPS license will enable either the Migration Accelerator (and Orchestrator) or the Insights or Monitor products within the suite.

When the application is first launched, a License ID is required to allow further configuration. This license ID should have been provided to you via email. If you have not received your license ID please contact pma.support@proventeq.com

NOTE: Proventeq is not responsible for providing the hardware, its maintenance, backups, or security management. Proventeq is not responsible for the software licenses, subscriptions, or the support for any 3rd party software described in this guide.

2.1. Application Server(s)

The application server is responsible for hosting the core engine and executing discovery, analysis, retrieval, data conversion and uploading. CPS Migration Accelerator can be designed to work on several systems, and this may increase overall throughput (depending upon environment bottlenecks). Contact Proventeq Sales (sales@proventeq.com) for pricing information.

The sections below describe the hardware, software and account pre-requisites that must be followed.

NOTE: To provide the best and most consistent performance it is recommended that the application server, staging database and source content system are located in the same Class C subnet.

2.1.1. Migration Accelerator Hardware requirements

The requirements below are based upon the amount of data to be migrated on a per server basis. For example, if the solution is to migrate 30 million items using two CPS application servers, then the solution would be to configure 2 servers using the medium migration requirements below.

Component	SMALL ¹ Migration (Up to 5 million items OR up to 1 TB data)	MEDIUM ¹ Migration (5 to 20 million items OR up to 4 TB data)	LARGE ¹ Migration (20 to 50 million items OR up to 10 TB data)
Processor	64-bit 4 vCPU	64-bit 8 vCPU or better	64-bit 16 vCPU or better
Memory (RAM)	16 GB	32 GB or higher	64 GB or higher
Data Storage ²	Solid-state disk: 500 GB free space	Solid-state disk: 750 GB free space	Solid-state disk: 1 TB free space
Network card ³	1 Gbps	1 Gbps	1 Gbps
Azure VM Size ⁴	Standard_D4_v5	Standard_D8_v5	Standard_D16_v5

1. May require more than 1 application server depending on volume of content and required throughput.
2. Storage requirement may vary depending on total migration volume or size. To migrate large files the minimum storage required will be 3 X size of largest file.
3. Minimum Network Bandwidth required is 100 Mbps.
4. Required only if provisioning in Azure cloud. VM sizes available at <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general>

NOTE: Failure to follow recommend hardware guidelines may result in slower migrations and increased migration timescales. In certain circumstances, making the operation of the migration unreliable.

2.1.2. Insights and Monitor Hardware Requirements

Component	Requirements
Processor	64-bit 8 vCPU
Memory (RAM)	32 GB or higher
Data Storage	Solid-state disk: 500 GB free space
Network card	1 Gbps
Azure VM Size ¹	Standard_D8_v5

Required only if provisioning in Azure cloud. VM sizes available at <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general>

NOTE: Failure to follow recommend hardware guidelines may result in slower data discovery and migration. In certain circumstances, making the product unreliable.

2.1.3. Software Requirements

This section covers the details of the software that's required on the CPS server.

Component	Requirement
Operating System	Windows Server 2016 x64 Standard or later
Additional software	• SQL Server Management Studio (SSMS)* (version corresponding to installed SQL server version) • Microsoft EDGE • If using Proventeq Insights product or Embedded Link Detection/Update in Migration Accelerator** ○ Microsoft Office 2019**** x86/x64 (Outlook, Word, Excel, PowerPoint) • Oracle SQL Developer or Oracle Client***
Visual C++ Redistributable	Visual C++ Redistributable
.NET framework 4.7.1 or later	Download Microsoft .NET Framework 4.7.1
PowerBI Desktop	Download PowerBI Desktop (Note: No license is required for PowerBI Desktop)
SQL Express 2019	Download SQL Express 2019 (for trials/small migrations)
If migrating from M-Files on-premise\cloud	https://www.m-files.com/customers/product-downloads/download-update-links/#online%20desktop%20only Select the relevant Desktop Only package.

*SQL Management studio (SSMS) is only required on the CPS server if remote access to the SQL server is not allowed.

**Feature which updates links within migrated document to correctly reflect the location of the new target location of other items to be migrated.

***Only required if source system uses Oracle databases and if access to an Oracle client on another server is not allowed.

**** Microsoft Office 2016 is supported but 2019 is recommended due to improved stability.

2.1.4. Source Specific licensing requirements

- Documentum - If using the Documentum API to retrieve data using the REST API a Documentum REST API is required.
- BOX - If migrating from BOX, contact your Box account Manager to discuss BOX API usage limits.
- CCH Axxess - If migrating from CCH Axxess, contact your CCH Axxess account Manager to discuss CCH Axxess API usage limits.

2.1.5. Network and Security

As Content Productivity Suite runs as an interactive desktop application, you should review and potentially adjust, policies related to automatic user session termination as these could otherwise terminate the application during migration.

For migrations to Office 365, it's recommended to have outbound network bandwidth of 1Gbps.

Discovery and migration activities require access to the relevant source and target environments from the application and database servers for discovery and migration activities, including accessing application URLs through browser, user interfaces (UI), client applications, APIs, databases, and file stores, from both the application and database servers as applicable.

2.1.5.1. Ports and Endpoint Requirement

Most content management systems have an underlying database (some Microsoft SQL, others support Oracle) and an underlying file system. For some systems there is only the products official API that allows the data to be accessed. For others, CPS may either use it's own access methods (and therefore require access to the underlying database and file system) or may still provide the option to use the API. So, these factors affect access permissions requirements and ports

Core Platform Port Requirements

Component	Port	Note
Staging database/ Source database ports	SQL Port 1433 (or 1434 if using SQL named instance)	Further information at https://docs.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access These are default ports but may be different in your environment
Endpoint for SharePoint/OneDrive migration	HTTP/HTTPS Ports 80 & 443	API Access to Office 365

Source Platform Specific Port Requirements

Source	Type	Note
Alfresco	HTTP	HTTP/HTTPS Ports 80 & 443
BOX	HTTPS	HTTP/HTTPS Ports 80 & 443
Documentum On-premise	HTTP or/and SQL and SMB	Port usage depends upon configuring settings If using API for Discovery and Migration > HTTP/HTTPS Ports 80 & 443 If NOT using API for Discovery and Migration Database connectivity Port 1433(TCP) & Port 1434 if using SQL named instance. (if Documentum using SQL) 1521 (if Documentum using Oracle) Item Retrieval Method If using API > HTTP/HTTPS Ports 80 & 443

		If using File Store retrieval method > Port 445(SMB) to allows access to underlying data to migrate
Exchange	HTTP	HTTP/HTTPS Ports 80 & 443
FileNet P8	HTTP & SQL	HTTP/HTTPS Ports 80 & 443 Port 1433(TCP) & Port 1434 if using SQL named instance. (if FileNet using SQL) 1521 (if FileNet using Oracle)
File Shares	SMB	Port 445(SMB) to allows access to underlying data to migrate
G-Suite/Google Workspace	HTTP	HTTP/HTTPS Ports 80 & 443
EDocs/Hummingbird	SQL and SMB	Port 1433(TCP) & Port 1434 if using SQL named instance.
iManage	SQL, SMB, HTTPS	Port 1433(TCP) & Port 1434 if using SQL named instance Port 445(SMB) to allows access to underlying data to migrate HTTP/HTTPS Ports 80 & 443 if migrating from/to iManage cloud instance
Meridio	SQL and SMB	Port 1433(TCP) & Port 1434 if using SQL named instance Port 445(SMB) to allows access to underlying data to migrate Allow access to Meridio database. Depending on the database (SQL Server, DB2, Oracle etc), ports and protocols could vary.
M-Files	HTTP	HTTP/HTTPS Ports 80 & 443
Oracle UCM	HTTP & SQL	HTTP/HTTPS Ports 80 & 443 Port 1433(TCP) & Port 1434 if using SQL named instance. (if Oracle UCM using SQL) 1521 (if Oracle UCM using Oracle)
OpenText Content Server	HTTP & SQL	HTTP/HTTPS Ports 80 & 443 Port 1433(TCP) & Port 1434 if using SQL named instance. (if Oracle UCM using SQL) 1521 (if Oracle UCM using Oracle)
ShareFile	HTTP	HTTP/HTTPS Ports 80 & 443
CCH	HTTP	HTTP/HTTPS Ports 80 & 443

OTCM	HTTP & SQL	HTTP/HTTPS Ports 80 & 443 Port 1433(TCP) & Port 1434 if using SQL named instance. (if Oracle UCM using SQL) 1521 (if Oracle UCM using Oracle)
------	------------	---

2.1.5.2. Anti-Virus Software

It's recommended that anti-virus software runs on the CPS system.

Folder Exclusions:

The following locations should be excluded from anti-virus scanning:

- **Installation folder:** Default is C:\Program Files\Proventeq\Proventeq Content Suite
- **Working folder:** Default is C:\Proventeq

Process Exclusions:

The following process should be excluded from anti-virus scanning

- Proventeq.ContentSuite.exe

2.1.5.3. Firewall Whitelist

Depending upon whether Migration Accelerator or Insights or Monitor is being used, the core server requires access to the following endpoints.

For browser-based SharePoint access and page rendering, client should also allow any additional Microsoft 365 endpoints required by the current Microsoft 365 URL and IP address range guidance, including authentication, CDN, Office web, and related SharePoint/OneDrive services.

The endpoints listed below represent the primary connectivity requirements. In addition, any dependent services or supporting endpoints, such as Content Delivery Networks (CDNs), image repositories, graphics services, authentication providers, and other third-party or application-specific dependencies, may also need to be whitelisted. The exact whitelist requirements can vary based on regional deployments, client security policies, network controls, and changes to application or system architecture at the time of prerequisite setup and migration execution.

Required Endpoint	Purpose	Migration Accelerator	Insights / Monitor
https://secure.aadcdn.microsoftonline-p.com	Microsoft 365 Authentication	Y	
https://login.microsoftonline.com	Microsoft 365 Authentication	Y	
https://api.office.com	Microsoft 365 APIs for content migration and validation	Y	
https://graph.windows.net	Microsoft 365 APIs for content migration and validation	Y	
https://graph.microsoft.com	Microsoft Graph API access	Y	Y

https://*.sharepoint.com	SharePoint Online / OneDrive target access	Y	Y
https://*.queue.core.windows.net	Azure Migration API Queue Storage	Y	
https://*.blob.core.windows.net	Azure Migration API Blob Storage	Y	
https://*.queue.core.usgovcloudapi.net	Azure Government Queue Storage	Y	
https://*.blob.core.usgovcloudapi.net	Azure Government Blob Storage	Y	
https://support.proventeq.com	Product documentation and support	Y	Y
https://licensing.proventeq.com	License activation	Y	Y
https://*.protection.outlook.com	Sensitivity Label processing	Y	
https://*.aadrm.com	Microsoft Purview Information Protection	Y	
https://*.azurerms.com	Microsoft Purview Information Protection	Y	
https://*.informationprotection.azure.com	Microsoft Purview Information Protection	Y	
https://ecn.dev.virtualearth.net	Microsoft Purview dependency	Y	
https://informationprotection.hosting.portal.azure.net	Microsoft Purview dependency	Y	
https://api.sharefile.com	ShareFile API access	Y	Y
https://*.sharefile.com	ShareFile content access	Y	Y
https://api.box.com	Box Content API	Y	Y
https://account.box.com	Box authentication	Y	Y
https://www.googleapis.com	Google Workspace / Google Drive API	Y	Y
https://accounts.google.com	Google OAuth authentication	Y	Y
https://admin.google.com	Google Workspace administration	Y	Y
https://cloudimanage.com	iManage Cloud content access	Y	Y
https://*.imanager.work	iManage Cloud APIs	Y	Y
https://api-docs/v2	iManage REST API (On-Prem)	Y	Y
https://wsi/FNCEWS40MTOM	FileNet Content Engine Web Services	Y	Y

<a href="http://*<Server>:8080/dctm-rest/services">http://*<Server>:8080/dctm-rest/services	Documentum REST API endpoint	Y	Y
https://*.alfresco.company.com/alfresco/api	Alfresco REST API	Y	Y
https://*.alfresco.company.com/alfresco/cmisaom	Alfresco CMIS API	Y	Y
https://*.opentext.company.com/otcs/cs.exe/api	OpenText Content Server REST API	Y	Y
https://*.mfiles.company.com/REST	M-Files REST API	Y	Y
https://*.oracleucm.company.com/idcplg	Oracle UCM / WebCenter Content API	Y	Y
https://api.cchaxcess.com	CCH Axxess API Service	Y	Y
https://login.cchaxcess.com	CCH Axxess authentication	Y	Y
https://outlook.office365.com	Exchange Public Folder access	Y	Y
https://*.otcm.company.com	OpenText Content Management API	Y	Y

2.2. CPS SQL Database Requirements

The SQL database associated with CPS is called the **Staging Database** and contains migration configuration, source metadata, processing and auditing information.

It's recommended that a dedicated SQL Server instance is used. An existing (shared) SQL Server instance for smaller migrations/trials located on the CPS server itself (subject to the specification meeting the criteria below) is supported but there will understandably be a performance impact.

NOTE: When configuring multiple CPS servers, each is required to have its own staging database.

The staging database can either be created during the installation or connected to a pre-created database during the installation.

Microsoft SQL Standard or Enterprise editions are supported for production and trials. Due to the performance and scale limitation of Microsoft SQL Express (Free) it is only supported for trials and small migrations.

Staging Database disk space sizing

Since the staging database contains a record for each item (and subsequent deltas) and associated metadata, the staging database size can be highly variable and so it's important to take steps to estimate it. We always recommend a pilot and during this, the number of items processed, and the size of the SQL database can collect and used to help estimate the SQL disk space requirements for a production migration would be.

2.2.1. SQL Hardware Requirements

A dedicated SQL instance can be provisioned using the following hardware requirements

Component	SMALL ¹ Migration (Up to 5 million items OR up to 1 TB data)	MEDIUM ¹ Migration (5 to 20 million items OR up to 4 TB data)	LARGE ¹ Migration (20 to 50 million items OR up to 10 TB data)
-----------	---	--	---

Processor	64-bit 4 vCPU	64-bit 8 vCPU or better	64-bit 16 vCPU or better
Memory (RAM)	16 GB	32 GB or higher	64 GB or higher
Data Storage ²	Solid-state disk: 500 GB free space	Solid-state disk: 750 GB free space	Solid-state disk: 1 TB free space
Network card ³	1 Gbps	1 Gbps	1 Gbps
Azure VM Size ⁴	Standard_D4_v5	Standard_D8_v5	Standard_D16_v5

1. May require more than 1 CPS application server and database server depending on volume of content and required throughput.
2. Storage requirement may vary depending on total migration volume or size.
3. Minimum Network Bandwidth required is 100 Mbps.
4. Required only if provisioning in Azure cloud. VM sizes available at <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general>

NOTE: Failure to follow recommend hardware guidelines may result in slower migrations and increased migration timescales. In certain circumstances, making the operation of the product unreliable.

2.2.2. Software Requirements

Component	Requirement
Operating System	Windows Server 2016 x64 Standard or later
Database	SQL Server Standard/Enterprise 2016 Sp1 or later (using CI, Case Insensitive collation)
Additional software	SQL Server Management Studio (SSMS) (version corresponding to installed SQL server version) SQL Native Client if TLS 1.0/1.1 is disabled

If using SQL Server Standard edition, the following configuration is recommended.

Number of cores /vCPU	Number of sockets	MAXDOP value (Setting on SQL Server)
4	1 socket of 4 cores	4
4	2 sockets of 2 cores each	2
8	1 socket of 8 cores	8
8	2 sockets of 4 cores each	4

16	2 sockets of 8 cores	8
----	----------------------	---

Other recommended settings for SQL Standard Server are:

Setting	Value
Cost threshold for parallelism	250 or above

2.3. Core Account Requirements

This section describes the different accounts that are required and relevant permissions.

System Name	User Accounts Requirements
Application Server	A Windows user account (also known as the Application Account) with local Administrator permissions to - Perform installation of software pre-requisites and Content Suite product. - Execute the migration
Database Server	Use Application Account for integrated authentication or a SQL Login account. This account will also be used by the application to access the database. If using integrated authentication to connect to SQL, grant the Application Account 'db_creator' permissions on the database server. If using SQL authentication to connect to SQL, grant the SQL Login account 'db_creator' permissions on the database server. Once the database has been created, it's possible to downgrade the permissions to db_datareader, db_datawriter and db_owner.
SharePoint Online ¹ 	An account with a license sufficient to allow it to access SharePoint. Proventeq Migration Accelerator App based authentication, where the Proventeq Migration Accelerator application ID can be used once the global administrator has granted admin consent. This Application ID uses delegated permission and hence requires a user with sufficient privileges to the target Site Collections. The Application Account requires Site Collection administrator privilege on all relevant target sites collections. NOTE: Conditional access feature on Azure Active Directory to bypass MFA for CPS servers may be required if MFA is enabled in customer tenancy.

¹ For Migration Accelerator only.

*Typically, the installation of CPS is done whilst logged into the Application account and the database is created during the installation process but if the account cannot be granted rights to create an SQL database, then it's possible for a blank database to be created manually and then during the installation of CPS it will connect to this database and set it up as required.

2.3.1. Source Specific User Account Requirements

In addition to core account requirements, there are additional account requirements depending upon the source system being migrated. For some sources, this may mean granting additional rights to the Application Account specified above, for others, typically API based, it may require access to the details of an account with such rights, which can be specified during configuration.

Source System	User Accounts Requirements
Alfresco	User having access to Alfresco CMIS API site to fetch data and perform migration. E.g. http://alfresco/cmisaom
Box	A Box account with administration rights. NOTE: When migrating from BOX, API calls are used to discover and retrieve data. This is likely to have an impact on the API limits associated with your BOX system. Therefore, it's essential to discuss your API call limits with your BOX Account Manager.
Documentum	There are two options for connecting to Documentum source. Option A means CPS will access the Documentum information at the database/disk level, Option B means CPS will access Documentum through API. Option A below allows for fastest migration but can only be used for On-Premise Documentum systems Option A: Direct Access The Application Accounts needs read permissions on source Documentum database (for using Integrated Authentication) or an SQL login account with read access. Read permissions for Windows user account (used on Migration Application Server) to access Documentum file store while performing migration. Option B: Using Documentum REST API (for on-premises version 7 and above, or hosted Documentum) A user account with privileges to fetch documents using the Documentum REST API. Allow access to the Documentum REST endpoint from the Application server. A Documentum REST API licence Note: For Documentum on-premises environment with encrypted file stores, a combination of Option A and Option B will be required. Basic Authentication method is used to access Documentum API. For more details on the Documentum REST API refer: Documentum REST API Developer Guide Note: For the migration of Documentum Virtual documents, the Document Sets feature in SharePoint must be enabled.
Exchange	User account with Read-only access to all Exchange Public Folders, which will enable the application to retrieve data.

FileNet P8	A FileNet user account with read privilege to invoke FileNet Content Engine Web Service API. This user will be used to access and retrieve FileNet metadata and content during migration. A user account on source FileNet database with read permissions on schema and data. This account is required if Migration Accelerator discovers content using the FileNet database. A user with access to FileNet client (Workplace XT). This user will be required to perform manual validation of content.
File Shares	The Application Account above, needs to have at least read access to File Share server to retrieve data.
G-Suite/Google Workspace	G-Suite system user account with admin permissions on G-Suite REST API Service. This user will be used to access and retrieve G-Suite metadata and contents during migration.
EDocs/Hummingbird	At least Read permissions for Windows user account (used on Migration Application Server) to access EDocs/Hummingbird File Share while performing migration.
iManage	A user account with 'db_reader' permissions on iManage Worksite database. For on-premises iManage: Windows user account with Read permissions to access iManage Worksite File Share while executing migration. For hosted iManage, or when file storage is encrypted: An iManage user account with privileges to retrieve files through the iManage REST API accessible at <a href="https://<YOURiManageSERVER>/api-docs/v2/#/docs/summary">https://<YOURiManageSERVER>/api-docs/v2/#/docs/summary (where <YOURiManageSERVER> is the actual name of your iManage server)
iManage Cloud	A user account with read and download access is required for the specified iManage cloud instance. Additionally, the Client ID and Secret must be provisioned as described in the reference article, and user-level access should be granted to these credentials to enable the invocation of the iManage API for content discovery and migration. Reference: https://docs.imanage.com/cloud/cc-help/en-US/Adding_an_application.html
Meridio	At least Read permissions for Windows user account (used on Migration Application Server) to access Meridio File Share while performing migration.
Oracle UCM	Oracle UCM user having access to UCM WebCenter content server/web service to perform migration configuration and execution.
OpenText CS	A user account with 'db_reader' permissions on OpenText Oracle/SQL database. An OpenText user account with privileges to retrieve files through the OpenText REST API service.

	A user account with access to the OpenText CS client (This is used for any manual verification of the content in Content Server).
ShareFile	ShareFile system user account with admin permissions ShareFile API key (Client ID and Client Secret) from https://api.sharefile.com/rest/ NOTE: If the environment uses MFA then it is essential to create an application specific password in ShareFile and use this as the connection password.
M-Files	M-Files user with named license or read-only type license. M-Files User having access of source vault.
PST	The Application account used for migration account needs to have at least write access to folder location to create the files at selected location.
SharePoint Online	Recommended option: App-Based Authentication For additional information on Azure application permissions and admin consent in the Microsoft identity platform endpoint, please refer to the link below. Overview of permissions and consent in the Microsoft identity platform - Microsoft identity platform... Please use the link below for details on how to obtain the TenantID for your organisation. https://learn.microsoft.com/en-us/sharepoint/find-your-office-365-tenant-id How to register Application ID: The whitelisted Application IDs for the migration are listed below. The Default CPS Application ID: d1e5e128-9660-4380-aabb-3e0061c1047c must be authorised on the tenant. If Sensitivity Labels are in use, the Application ID should be 0a8da96c-bf61-4839-9ede-2d0b6647414c To register the Application ID, use the URLs below and replace the actual Tenant ID in the URL <TenantID>. If the user is a Global admin user, they will see a consent screen and need to accept the consent. Select the checkbox to grant consent on behalf of your organisation, then click the “Accept” button. If the user is not a Global Admin, they will need to ask an Admin user to log in and accept the consent for Proventeq Migration Accelerator application. Standard <a href="https://login.microsoftonline.com/<TenantID>/adminconsent?client_id=d1e5e128-9660-4380-aabb-3e0061c...">https://login.microsoftonline.com/<TenantID>/adminconsent?client_id=d1e5e128-9660-4380-aabb-3e0061c... If using Sensitivity Labels <a href="https://login.microsoftonline.com/<TenantID>/adminconsent?client_id=0a8da96c-bf61-4839-9ede-2d0b664...">https://login.microsoftonline.com/<TenantID>/adminconsent?client_id=0a8da96c-bf61-4839-9ede-2d0b664...

	The service account used for the connection must be added as a SharePoint Admin or as an owner of all site collections.
OneDrive	The migration service account must have OneDrive admin access. If the source OneDrive belongs to a different account, add the service account as a secondary administrator.
CCH	A dedicated CCH Axxess service account with the CCHAccess_data_writeaccess and offline_access permissions enabled on the CCH Axxess API Service is required. This account will be used by the migration process to authenticate with the CCH Axxess API and retrieve metadata and content from the source system.
OCTM	A user account with 'db_reader' permissions on OTCS Oracle/SQL database. An OpenText user account with privileges to retrieve files through the OpenText REST API service. A user account with access to the OTCS client (This is used for any manual verification of the content in Content Server).

3. SHAREPOINT GRAPH DISCOVERY PREREQUISITES

To configure graph discovery to run against the tenant, use following steps to set it up.

3.1. Create an App Registration in Azure Portal

For app Registration on azure portal, refer this link: <https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-register-app#register-an-application>

3.2. Add Permissions to the application

For setting up app permissions to allow running graph discovery, follow the steps below

3.2.1. Graph API Permissions

1. In the app registration page, select **API permissions** from the left-hand menu.
2. Click on Add a permission.
3. Choose Microsoft Graph.
4. Choose Application permission. Search for and select Sites.Read.All.
5. Click Add permissions.
6. Click on Grant admin consent for [Your Organization] to grant the permissions.

NOTE: The Graph API **Sites.Read.All** application permission is the least privileged permission required for the Monitor tool to do any Graph API Request. Without this permission, the tool will not be able to function.

3.2.2. REST API Permissions

1. Click on Add a permission.
2. Choose SharePoint.
3. Choose Application permission. Search for and select Sites.FullControl.All.
4. Click Add permissions.
5. Click on Grant admin consent for [Your Organization] to grant the permissions.

NOTE: The SharePoint **Sites.FullControl.All** application permission is the least privileged permission required for the Monitor tool to be able to retrieve the permissions of SharePoint items. If this permission is not given, the tool will not be able to do REST requests for fetching permissions and **none of the item security will be discovered**.

3.3. Generate Certificate

CPS requires a .pfx file to perform graph discovery. For that, follow the steps below.

Step 1: Generate public certificate

To generate public certificate, refer to this link: [Create a self-signed public certificate to authenticate your application - Microsoft identity platform | Microsoft Learn](#)

Step 2: Generate pfx file

Generate the certificate without a password and save it with the .pfx extension once the certificate file has been generated, refer to this link: [Create a self-signed public certificate to authenticate your application - Microsoft identity platform | Microsoft Learn](#)

Step 3: Upload Certificate

Once .cer file is generated, use this link to upload that into Azure: [Add and manage app credentials in Microsoft Entra ID - Microsoft identity platform | Microsoft Learn](#)

NOTE: Application permissions are preferred over Delegated permissions as we are running as a service and not in the context of a user. There are also limitations using Delegated permissions over Application permissions in some of the Graph and SharePoint API Calls. Certificates are preferred over Client Secret, because Microsoft do not allow you to connect to the Graph and REST API using that type of authentication. More information about this can be found [here](#).

4. GOOGLE WORKSPACE PREREQUISITES

To perform Google Workspace discovery and migration, complete the required setup steps, including creating a service account, configuring domain-wide delegation, and generating a JSON key file. Refer to the table below for the steps to configure the Google service account and generate the JSON key.

Step	Step Description	Reference Documentation
1	Create a new project. For that navigate to this URL - Google Cloud Platform	Create projects
2	Select above created project from project selector for further configuration	
3	Enable Admin SDK API from API Library	Enable Google Workspace APIs
4	Enable Google Drive API from API Library	Enable Google Workspace APIs
5	Go to APIs & Services > Credentials and Create a Service Account using this URL- https://console.cloud.google.com/apis/credentials	Create service accounts
6	Open the created service account > Advanced settings > copy the Client ID Google Cloud Platform	
7	Go to Google Workspace Admin Console using https://admin.google.com/ URL and configure Domain-Wide Delegation. Add the following OAuth scopes : Scope 1 (Admin SDK read-only Access): https://www.googleapis.com/auth/admin.directory.user.readonly Scope 2 (Google Drive access): https://www.googleapis.com/auth/drive	Control API access with domain-wide delegation
8	Update IAM policy (iam.disableServiceAccountKeyCreation) in case its not enable using this URL - Google Cloud Platform	Troubleshoot organization policy errors for service accounts
9	Go back to Service Account using this URL - https://console.cloud.google.com/iam-admin/serviceaccounts > Keys > Create JSON key and download it.	Create and delete service account keys

5. STAGING DATABASE BEST PRACTICES AND GUIDELINES

To ensure optimal performance, stability, and reliability of the Proventeq V9 platform, it is important to follow a set of operational best practices during discovery and migration activities. These recommendations help minimize database contention, reduce the likelihood of performance bottlenecks, and ensure that supporting infrastructure remains healthy throughout migration workloads. Adhering to these guidelines can improve overall system efficiency and simplify troubleshooting if issues occur.

1. **Avoid Using Shared SQL Server Instances for Migration Workloads**

Where possible, use a dedicated SQL Server instance for Proventeq discovery and migration activities rather than sharing the instance with other business-critical applications or services. Shared SQL Server environments can introduce resource contention across CPU, memory, storage, and I/O subsystems, potentially affecting migration throughput and stability. A dedicated SQL Server instance helps ensure predictable performance, simplifies capacity planning, and reduces the risk of external workloads impacting migration operations.

2. **Schedule SQL Server Maintenance Carefully**

Ensure that SQL Server maintenance activities, such as scheduled backups, index rebuilds, and integrity checks, are planned to avoid overlapping with discovery or migration operations. Running these tasks concurrently can increase resource contention and negatively impact migration performance.

3. **Implement Regular Index Maintenance**

Proventeq provides an application setting to automate index rebuilds. If this feature is not enabled, schedule regular index maintenance during periods when no discovery or migration jobs are running. Maintaining healthy indexes helps ensure consistent database performance.

4. **Limit Backend Database Activity During Migrations**

Avoid executing migration database reports, ad hoc SQL queries, or other backend database activities while discovery or migration processes are in progress. Additional database workloads can increase latency and affect processing throughput.

5. **Monitor SQL Server Health and Performance**

Continuously monitor key SQL Server performance metrics during discovery and migration runs, including CPU utilization, memory consumption, disk latency, TempDB usage, and active database sessions. Proactive monitoring helps identify potential bottlenecks before they impact operations.

6. **Plan for TempDB Capacity Requirements**

For SharePoint Online (SPO) Graph Discovery, ensure that sufficient SQL TempDB storage capacity is allocated based on the expected workload size. Inadequate TempDB resources can lead to slower processing and unexpected job failures.

7. **Maintain Stable Infrastructure Connectivity**

Ensure reliable network connectivity between migration servers, the SQL Server environment, and source systems throughout discovery and migration activities. Network interruptions can cause delays, retries, or failed operations.

8. Retain Diagnostic Logs for Troubleshooting

Preserve relevant Windows Event Logs, SQL Server Error Logs, and Proventeq application logs. These logs are essential for troubleshooting and root-cause analysis should any issues need to be investigated after migration activities have completed.

9. Minimize Dashboard and Reporting Access During Active Jobs

Avoid accessing dashboards, reports, or other monitoring screens while discovery or migration jobs are actively running. Where possible, allow jobs to complete before opening detailed views of the same workload. This helps reduce resource contention, lowers the risk of database deadlocks, and prevents application thread stalls that could affect job execution.

10. Validate Environment Health Before Large-Scale Operations

Before initiating large discovery or migration workloads, verify that the database environment, operating system resources, and network infrastructure are operating within normal thresholds. A pre-run health check can help prevent avoidable disruptions and improve overall migration reliability.

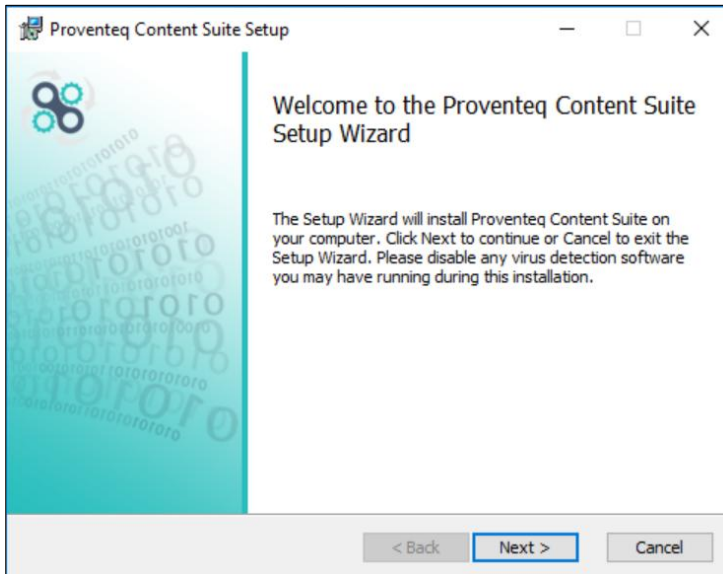
6. INSTALLATION

This section describes the steps involved during the actual installation of the content suite software.

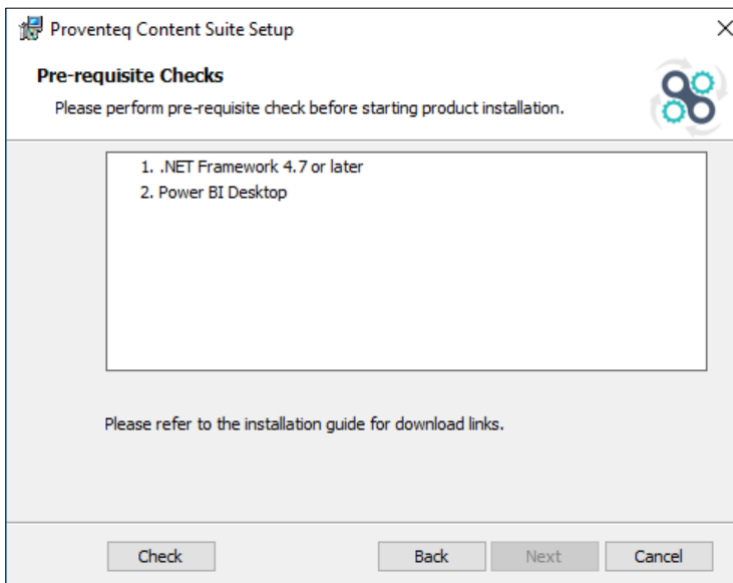
New Installation

To begin the installation, log in as the CPS Application Account and execute Proventeq.MigrationAccelerator.Setup.exe, with **“Run as administrator”** option.

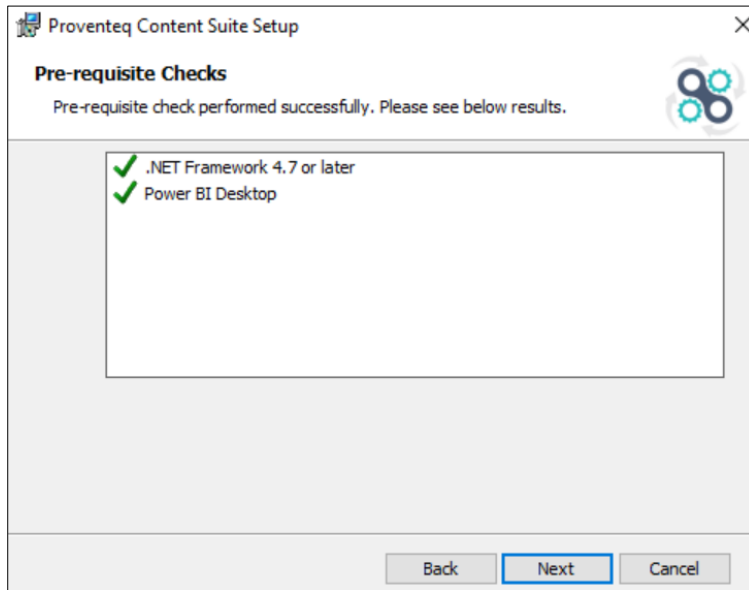
6.1. Welcome Screen



6.2. Pre-requisite Checks



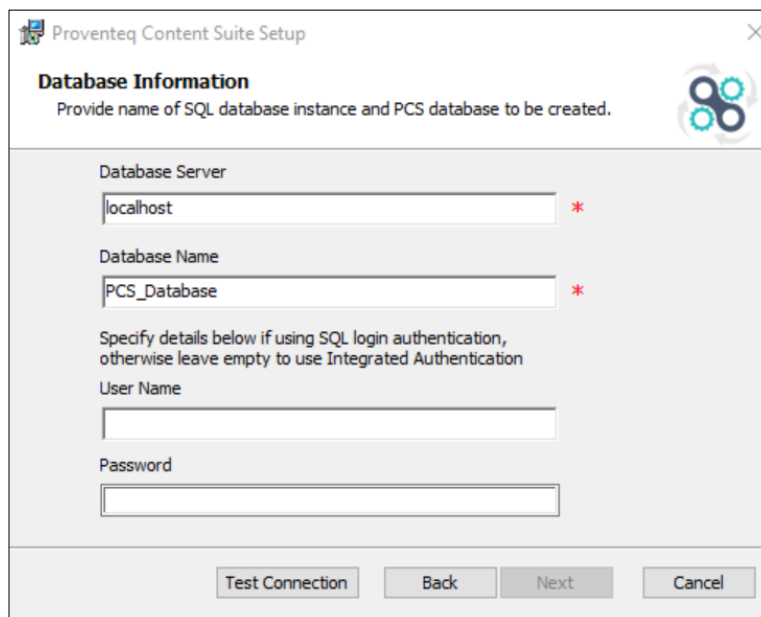
The screen above displays the software pre-requisites, click the Check button to carry out tests to confirm they are installed. After the checks, a screen similar to below will appear. Any software missing will have a red X next to them. If there are any failures review the pre-requisites list shown above and if that does not resolve the issue, follow the steps in the troubleshooting section below.



Click on Next button.

6.3. Database Information

CPS requires its own SQL database which will be created during the installation. Specify the SQL server to host the database and the name you wish to use for this database.



New Installation:

Enter the SQL Server name and a name you want to give for the CPS Staging Database.

Note: If using SQL Express, the default installation will create an SQL Instance so use a format like localhost\SQLEXPRESS

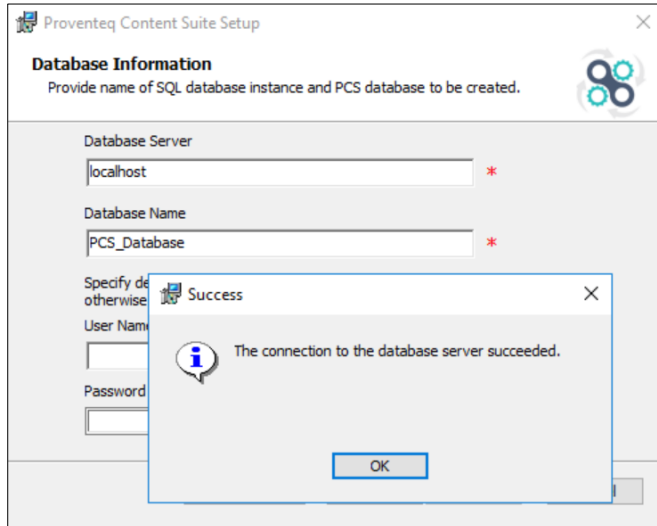
If using non default ports then syntax is <SQLserver>\<Instance Name>,<Port number>

Upgrade Installation:

Enter the SQL Server name and the name of the CPS Staging Database that was previously created.

NOTE: Only specify a Username and Password if you wish to use SQL authentication method. Leave these fields blank to use integrated security. The account logged into will be used to create the database and access it going forwards.

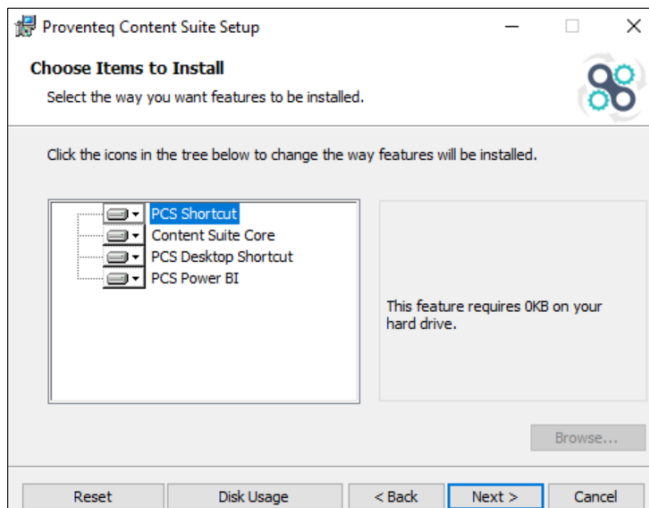
Click on “Test Connection” to verify SQL details and then the screen below will appear.



Click on Next button.

6.4. Choose Items to Install

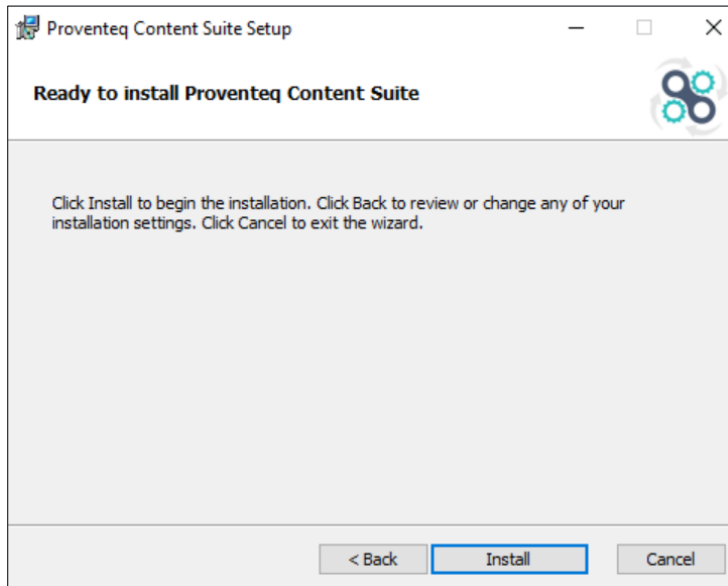
Click Next to display the Choose Items to Display screen



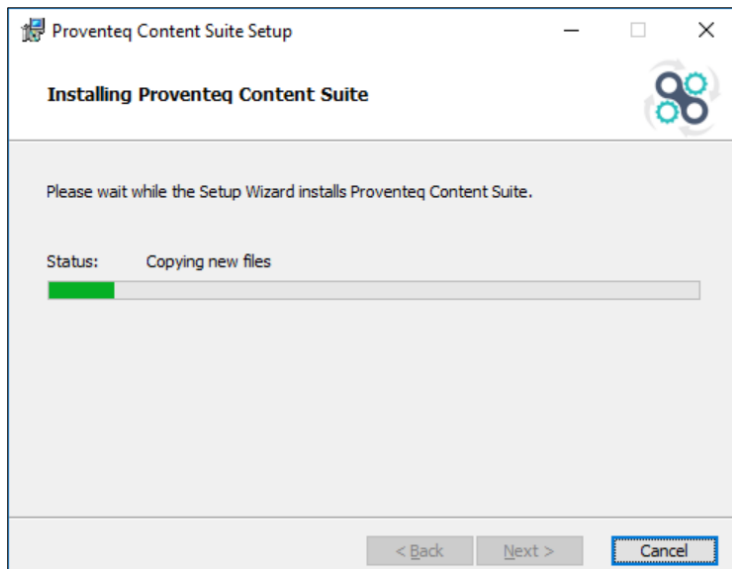
If required change location for feature(s) to install by clicking on Browse button, the default is normally fine.

6.5. Confirm and Complete Installation

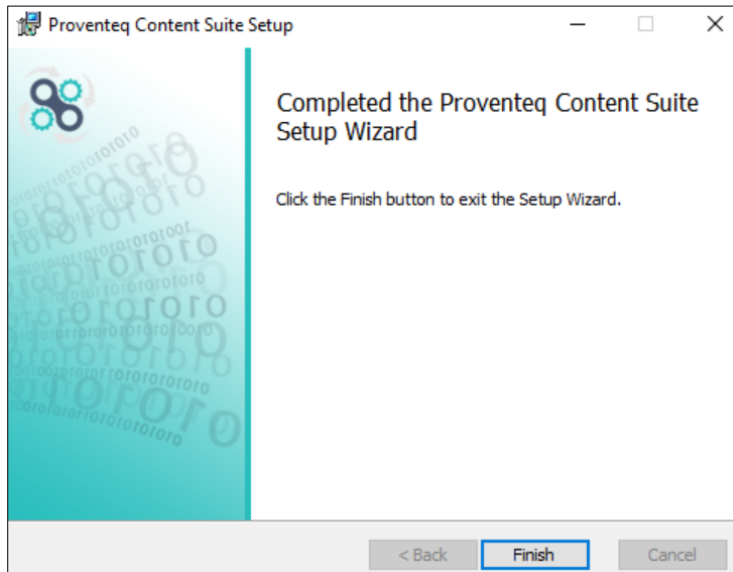
Click Next to display the Ready to install Content Productivity Suite screen



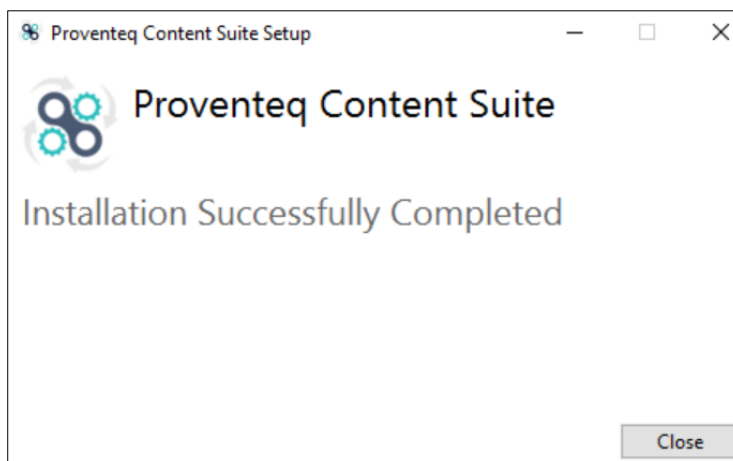
Click on Install to begin installation



On completion of Installation below setup completion screen will be displayed



Click Finish.



Click Close. This completes the installation process.

6.6. Troubleshooting Installation Problems

During the installation process two diagnostic logs files are created called **Proventeq_Migration_Accelerator_*.log** in %TEMP% folder and **C:\log.txt**. If a failure occurs during installation, review these log files for errors to identify possible cause or send them to Proventeq Technical Support for further analysis.

6.7. SharePoint Online Graph discovery Tool Setup

1. Extract the Graph Discovery Tool installation package.
2. Copy all files and folders from the extracted installer package.
3. Navigate to the Proventeq Content Suite installation directory: "*C:\Program Files\Proventeq\Proventeq Content Suite\GraphDiscoveryTool*"
4. Paste the copied files into the **GraphDiscoveryTool** folder.
5. If prompted, select **Replace the files in the destination** to overwrite existing files.

7. LAUNCH APPLICATION

Now, launch the application from **Desktop** by double clicking Content Productivity Suite icon

OR

Click from **Start -> All Programs -> Proventeq Content Suite -> Proventeq Content Suite**

After starting the application for the first time, you'll be required to activate the license. License activation help can be found in the CPS User Guide.

8. UPGRADE/UNINSTALL THE SOFTWARE

8.1. Upgrade process

The process to upgrade CPS is to first uninstall the existing version before then installing the new release.

IMPORTANT

If changes have been made to any CPS configuration files (i.e. *.exe.config files) then prior to the uninstall, take a backup copy of these *.exe.config files from the CPS installation directory and contact CPS support for advise on whether such changes will need to be reapplied once the software has been upgraded.

8.2. Uninstall Software

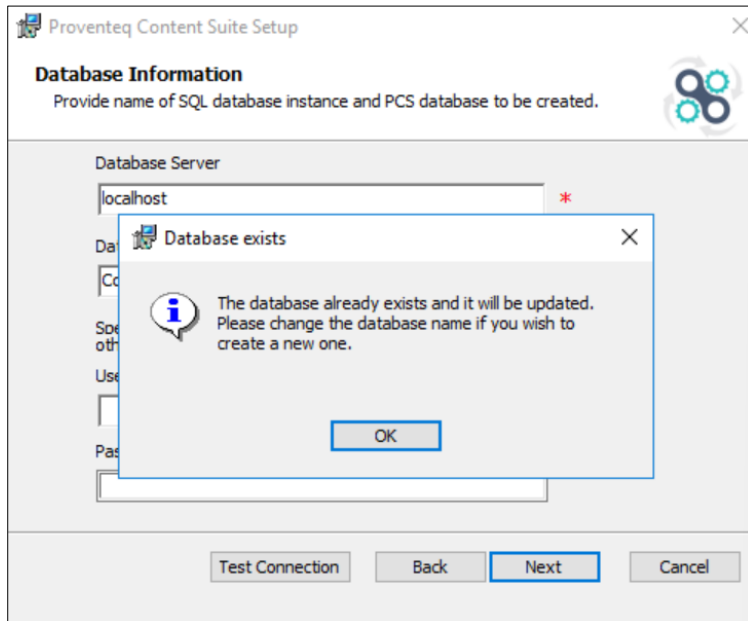
To uninstall the Proventeq Content Suite:

1. Close all applications and windows before proceeding.
2. Select **Start -> Control Panel**
3. Click on **“Uninstall a program”** under Programs option. Note: If you receive the message stating that you need administrator rights or privileges, log off the computer, then log on again as a user with administrator privileges.
4. Select Proventeq Content Suite
5. Click Change/Remove to start uninstallation process
6. At the prompt, click OK to confirm uninstall.

8.3. Installing upgraded software

Once the previous release has been uninstalled, run the installation procedure as described above and when prompted for database information, specify the name of the CPS database that was created originally.

The following message will be displayed to confirm that the existing database has been found, and CPS will then automatically carry out steps to upgrade the database as necessary.



IMPORTANT: If the above message is not displayed then the installation will be treated as a new, clean installation. In that case, exit the installation and find the correct database name and repeat installation process.

8.4. SharePoint Online Graph discovery Tool Setup

1. Extract the Graph Discovery Tool installation package.
2. Copy all files and folders from the extracted installer package.
3. Navigate to the Proventeq Content Suite installation directory: "C:\Program Files\Proventeq\Proventeq Content Suite\GraphDiscoveryTool"
4. Paste the copied files into the **GraphDiscoveryTool** folder.
5. If prompted, select **Replace the files in the destination** to overwrite existing files.