

ControlPoint

Software Version 5.9.0

Installation Guide



Document Release Date: April 2022
Software Release Date: August 2020

Legal notices

© Copyright 2016-2022 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for updated documentation, visit <https://www.microfocus.com/support-and-services/documentation/>.

Support

Visit the [MySupport portal](#) to access contact information and details about the products, services, and support that Micro Focus offers.

This portal also provides customer self-solve capabilities. It gives you a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the MySupport portal to:

- View information about all services that Support offers
- Submit and track service requests
- Contact customer support
- Search for knowledge documents of interest
- View software vulnerability alerts
- Enter into discussions with other software customers
- Download software patches
- Manage software licenses, downloads, and support contracts

Many areas of the portal require you to sign in. If you need an account, you can create one when prompted to sign in.

Contents

Chapter 1: ControlPoint overview	8
ControlPoint product suite	8
The Micro Focus IDOL platform	8
ControlPoint architecture	9
ControlPoint components	9
Chapter 2: Installation overview	13
Plan your ControlPoint deployment	13
Sample ControlPoint topology	14
Size and scale considerations for IDOL content	15
Chapter 3: Install SQL Server	16
Install SQL Server software	16
Configure SQL Server memory options	16
Set the Windows power plan for the server	17
Chapter 4: Install ControlPoint databases	18
ControlPoint databases	18
Database overview	18
Benefits of database partitions and file groups	19
Logical file groups	19
File groups example	20
Prepare to install ControlPoint databases	20
Verify the SQL Server sa account	20
Configure minimum SQL permissions	21
Grant permissions on database file locations	21
Start the SQL Server Agent service	21
Configure the ControlPoint data source	21
Install the ControlPoint databases	23
Perform post-installation database tasks	26
Move the ControlPoint databases	26
Configure the recovery model for ControlPoint databases	27
Chapter 5: Install ControlPoint IDOL and connectors	28
Create deployment packages	28

Configure deployment packages	29
Save deployment package configuration	33
Build deployment packages	33
Install deployment packages	33
Complete the Content Manager connector installation	34
Configure the Documentum connector	35
Set up IDOL Content language types	35
Start Windows services	35
Stop Windows services	36
Deploy multiple MetaStore services	36
Overview	37
Prepare for deployment	38
Deploy the additional MetaStore component	39
Modify the Install and Uninstall MetaStore scripts	39
Modify the Install Services script	40
Modify the Start Services script	40
Modify the Stop Services script	41
Associate Connector Framework Services (CFS) to the new MetaStore component	41
Uninstall deployment packages	41
Chapter 6: Install ControlPoint components	43
Enable Federal Information Processing Standards (FIPS) security mode	43
Limitations	44
Enable FIPS	44
Install ControlPoint and the ControlPoint Engine	44
Configure ControlPoint	45
Deploy ControlPoint by enabling HTTPS	50
Enable HTTPS	50
Create certificates	50
Configure certificate usage in IIS Manager	51
Update ControlPoint component configuration files	52
Redeploy ControlPoint when HTTPS is enabled	54
Configure the Redirector service for HTTPS	54
Create certificates	54
Bind certificate with a port	55
Configure the Redirector service for HTTPS	55
Chapter 7: Install the ControlPoint Edge File System connector	57
Install ControlPoint Edge File System Connector software	57
Configure the Edge File System Connector for HTTPS	58

Uninstall the Edge File System connector	59
Chapter 8: Optimize IDOL configuration	60
Chapter 9: Configure IDOL for HTTPS	62
Configure IDOL and connectors for HTTPS	62
Create SSL certificates	62
Update the IDOL configuration	62
Configure ControlPoint to enable IDOL in HTTPS mode	71
Stop IDOL services running with HTTPS	73
Run ControlPoint Configuration Manager with HTTPS enabled	74
Troubleshooting	74
Chapter 10: Set up IDOL distributed mirror / non-mirror modes	77
Introduction	77
Set up mirror mode	77
Set up non-mirror simple combinator mode	78
Add exception in Windows Firewall	83
Chapter 11: Adjust antivirus software monitoring	84
Chapter 12: Update DataAnalysis configurations after IIS hardening	85
Chapter 13: Upgrade ControlPoint	86
Run the Support utility	86
Note the current databases	87
Deactivate deprecated connectors	87
Prepare the ControlPoint environment for upgrade	88
Uninstall the current ControlPoint software	90
Upgrade to ControlPoint 5.9.0 software	90
Upgrade ControlPoint databases to 5.9.0	91
Prepare to upgrade ControlPoint databases	92
Verify the SQL Server sa account	92
Configure minimum SQL permissions	92
Grant permissions on database file locations	92
Determine whether a DockKey update is required	93
Upgrade the databases to 5.9.0	93
Database post-upgrade tasks	96
Move ControlPoint databases	96

Perform DockKey update	97
Configure the recovery model for ControlPoint databases	99
Consider ControlPoint database partitioning and file groups	99
Install the ControlPoint software	100
Upgrade IDOL data and software	100
Complete the IDOL software upgrade manually	101
Update configuration files	102
Update configuration files for DockKey update	102
Update Connector configuration files	103
Update Insert Configuration files	106
Update Insert Configurations for Content Manager connectors	106
Update IDOL files (new IDOL locations only)	107
Reconfigure the Documentum connector	108
Perform post-upgrade steps	108
Rescan repositories having custom properties	110
Upgrade the ControlPoint Edge File System Connector	111
Configure the ControlPoint Edge File System Connector for HTTPS	112
Upgrade NiFi IDOL Ingest libraries	112
Chapter 14: Configure Advanced IDOL Distribution	115
Chapter 15: Troubleshooting	122
Connectors	122
Edge Filesystem connectors	127
SharePoint connectors	127
Content Manager connectors	127
Compact stored procedure	128
Diagnostics logs	130
Policy execution logs	130
Data Analysis logs	131
Data Analysis service logs	131
Data Analysis Controller logs	131
Statistics Export utility trace logs	132
IDOL	132
Remote connectors	132
HTTPS setup for IDOL	133
IDOL distributed mirror / non-mirror setup	135
Policy execution	135
Proxy server interactions	138

Chapter 16: Metadata ingestion	140
Data mapping	140
MetaStore.MapColumn	140
MetaStore.MapTable	141
MetaStore.MapField	142
Additional data capture	143
Examples	143
Example 1: Single value for the same document	144
Example 2: Single value hash for the same document	144
Example 3: Multiple values for the same document	146
Example 4: Multiple values hashed for the same document	147
Existing data and re-ingestion	148
Field text and advanced properties	149
Field text	149
Properties and advanced properties	150
Chapter 17: ControlPoint multi-domain configuration	151
Prerequisites	151
Configure multi-domain support	152
Test your multi-domain configuration	155
Appendix A: ControlPoint Support utility	156
Appendix B: Configure ControlPoint security settings	158
ControlPoint IDOL configuration	158
ControlPoint OGS configuration	159
Documentum Connector configuration	160
Filesystem Connector configuration	161
SharePoint Remote Connector configuration	161
Appendix C: Configure ControlPoint with IDOL Media Server	162
Send documentation feedback	165

Chapter 1: ControlPoint overview

This chapter provides an overview of Micro Focus ControlPoint.

- [ControlPoint product suite](#)
- [The Micro Focus IDOL platform](#)
- [ControlPoint architecture](#)
- [ControlPoint components](#)

ControlPoint product suite

ControlPoint delivers a broad set of features targeted at addressing information management and governance challenges within the enterprise.

- **Break the silos of information.** Break down information silos and enforce consistent information governance across the entire corporate infrastructure. ControlPoint helps you achieve this using its inbuilt connectivity to the most commonly used data repositories and its capability to address many others.
- **Apply information lifecycle management.** Analyze all your documents to determine if they hold business value, constitute a record, or hold no value. Identify orphaned and unknown data. Develop a taxonomy and apply a complex policy to impose the most appropriate retention to each document.
- **Enforce compliance and security.** Use the ControlPoint analysis and entity extraction capability to identify potentially sensitive documents that need to be protected. Leverage the available policies to ensure that all the documents are properly secured in the desired locations.
- **Optimize storage and application performance.** Manage and delete data that hold no value. Implement a hierarchical storage management strategy to ensure a better utilization of your storage and to improve your backup and application performance.

ControlPoint enables you to understand the value of your data, and thereby gain control of your valuable information and achieve better data management.

The Micro Focus IDOL platform

For the purposes of full text analysis, ControlPoint utilizes the Micro Focus *Intelligent Data Operating Layer* (IDOL), which gathers and processes unstructured, semi-structured, and structured information in any format from multiple repositories using a global relational index.

As a next step, IDOL forms a contextual understanding of the information in real time, connecting disparate data sources together based on the concepts contained within them. For example, IDOL can automatically link concepts contained in an email message to a recorded phone conversation,

which can be associated with a stock trade. This information is then imported into a format that is easily searched, adding advanced retrieval, collaboration, and personalization to any application that integrates the technology.

For more information on IDOL, see the *IDOL Concepts Guide* and the *IDOL Server Getting Started Guide*, available from the [Micro Focus IDOL documentation site](#).

ControlPoint architecture

ControlPoint has a web application user interface. Functionality is available through several Dashboards in the user interface.

ControlPoint components

ControlPoint includes the following components:

- [ControlPoint Dashboard](#)
- [ControlPoint Engine](#)
- [ControlPoint Data Analysis](#)
- [ControlPoint IDOL](#)
- [ControlPoint Database](#)
- [ControlPoint MetaStore](#)
- [ControlPoint Redirector](#)
- [ControlPoint Connectors](#)

ControlPoint Dashboard

The ControlPoint Dashboard interface allows users to view repositories, establish and review policy allocation, administer Micro Focus IDOL categories, and monitor system activity and health, depending on their roles. It consists of the following services:

- **ControlPoint Web Interface.** IIS web application that serves as the ControlPoint user interface.
- **ControlPoint Web Service (Optional).** ControlPoint Web Service (CPWS), which provides the Edge connector access to Edge policies and configuration.

ControlPoint Engine

The ControlPoint Engine provides the central capability to manage policy content within an organization. It consists of the following services:

- **ControlPoint Engine service.** Windows service that executes all scheduled tasks.
- **CallbackHandler.** IIS web application that receives notifications from IDOL connectors.
- **ControlPoint LicenseService.** Windows service that tracks the data usage details of your ControlPoint environment. The data populates the Usage Details page in the ControlPoint Dashboard.

This service is separate from the ControlPoint License Server service packaged with ControlPoint, which controls IDOL licensing.

ControlPoint Data Analysis

ControlPoint Data Analysis allows your organization to analyze and understand, and to deal with the unstructured data contained within legacy repositories. ControlPoint uses IDOL connectors to scan and capture metadata and (optionally) content of files in the repository to analyze them, and then to present the results of the statistical analysis visually in a dynamic user interface.

ControlPoint IDOL

ControlPoint IDOL delivers an analysis of all content that ControlPoint manages. All repositories that are to be considered by ControlPoint for policy application must be scanned into IDOL.

The ControlPoint IDOL Deploy Tool can deploy the following items:

- **ControlPoint IDOL service.** Contains the central index.
- **ControlPoint Content services.** Index all of the content and serves search requests.
- **ControlPoint Content Manager Trim connector service.** Scans and performs actions on items in Content Manager repositories. This connector type has a connector framework deployed alongside.
- **ControlPoint DataAnalysis Store service.** Analyzes, understands, and deals with the unstructured data contained in legacy repositories.
- **ControlPoint Distributed connector service.** Distributes connector calls to the appropriate connector.
- **ControlPoint Documentum connector service.** Scans and performs actions on items in Documentum repositories.
- **ControlPoint Exchange connector service.** Scans and performs actions on items in Exchange repositories.
- **ControlPoint FileSystem connector service.** Scans and performs actions on items in file shares.
- **ControlPoint Hadoop connector service.** Scans and performs actions on items in Hadoop repositories.
- **ControlPoint IDOL License Server service.** Controls the licensing of all ControlPoint functionality.

- **ControlPoint OGS (Omni Group Server) service.** Collects and aggregates user and group security information from a variety of repositories.
- **ControlPoint Notes connector service.** Scans and performs actions on items on a Notes server.
- **ControlPoint SharePoint Remote connector service.** Scans and performs actions on items in SharePoint and SharePoint Remote sites.

ControlPoint Database

The ControlPoint Database provide storage for all policies, repository definitions, configuration settings, schedule tasks, and security information.

ControlPoint MetaStore

ControlPoint MetaStore is a relational database used to store information about all files in repositories that are being managed or analyzed by ControlPoint. Information stored includes document and repository metadata such as file create date, document author, and so on. Policy execution status is also stored in ControlPoint MetaStore.

ControlPoint Redirector

ControlPoint Redirector service retrieves file contents when a shortcut established by a Secure Shortcut policy is clicked.

ControlPoint Connectors

ControlPoint connectors and accompanying connector framework services scan and extract metadata and (optionally) content from files in source repositories. Connectors are also used to action policy execution instructions such as dispose or secure.

Connectors are specific to the repository type. The following connectors are provided with ControlPoint:

- **ControlPoint Content Manager connector.** Scans and performs actions on items in Content Manager repositories. This connector type has a connector framework deployed alongside.
- **ControlPoint Distributed connector.** Distributes connector calls to the appropriate connector.
- **ControlPoint Documentum connector.** Scans and performs actions on items in Documentum repositories. This connector type has a connector framework deployed alongside.
- **ControlPoint Edge Filesystem connector.** Scans and performs actions on items in file shares. This connector type has a connector framework deployed alongside.

- **ControlPoint Exchange connector.** Scans and performs actions on items in Exchange repositories. This connector type has a connector framework deployed alongside.
- **ControlPoint FileSystem connector.** Scans and performs actions on items in file shares. This connector type has a connector framework deployed alongside.
- **ControlPoint Hadoop connector.** Scans and performs actions on items in Hadoop repositories. This connector type has a connector framework deployed alongside.
- **ControlPoint Notes connector.** Scans and executes policy on messages, appointments, contacts, and other items from a Notes server. This connector type has a connector framework deployed alongside.
- **ControlPoint SharePoint Remote connector** scans and performs actions on items in SharePoint and SharePoint Remote sites. This connector type has a connector framework deployed alongside.

Chapter 2: Installation overview

The ControlPoint installation process consists of installing and configuring several different types of components in your environment.

The following tasks provide a broad overview of the tasks required to install ControlPoint:

1. Review the *ControlPoint Support Matrix*, available from the [Micro Focus ControlPoint documentation site](#), and ensure your environment meets all requirements.

As the *Support Matrix* notes, ControlPoint provides some required software in the ControlPoint IDOL deployment packages you create. If you want to install that software now, download a copy of it from the Internet. Otherwise, you can wait until after you create the deployment packages and it becomes available.

2. [Plan your ControlPoint deployment.](#)

Before installing ControlPoint, plan the topology and identify IDOL content size and scale considerations for maximum performance.

3. [Install SQL Server.](#)

4. [Install ControlPoint databases.](#)

5. [Install ControlPoint IDOL and connectors](#) using the included Deploy Tool package.

6. [Install ControlPoint components.](#)

7. [Install the ControlPoint Edge File System connector.](#)

8. (Optional) [Optimize IDOL configuration.](#)

9. (Optional) [Configure IDOL for HTTPS.](#)

10. (Optional) [Set up IDOL distributed mirror / non-mirror modes.](#)

11. [Adjust antivirus software monitoring.](#)

There are adjustments you can make to prevent antivirus software from impacting the performance of ControlPoint host machines.

12. If you enabled the Extended Protection for Authentication mechanism in IIS for your DataAnalysis service, [update DataAnalysis configurations.](#)

This step ensures that you can access repositories through ControlPoint.

Plan your ControlPoint deployment

To maximize the performance of your ControlPoint environment, think about its topology and review size and scale considerations for IDOL content before starting to install ControlPoint.

The following topics provide information in these areas:

- [Sample ControlPoint topology](#)
- [Size and scale considerations for IDOL content](#)

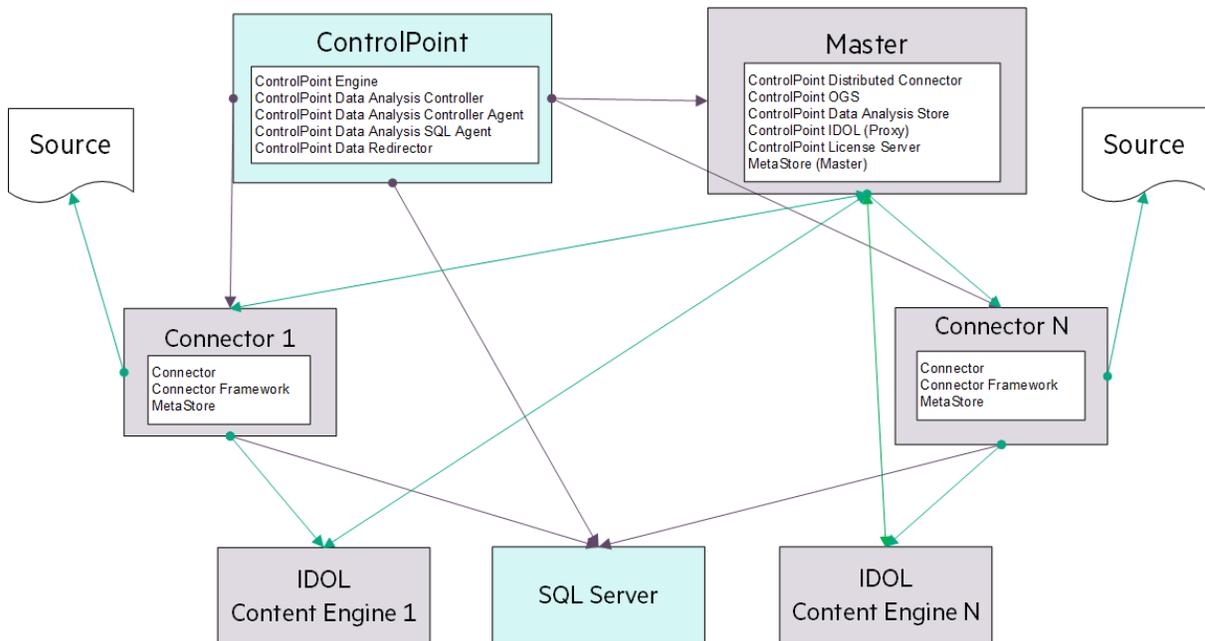
If you have any questions while planning your ControlPoint environment, contact Micro Focus ControlPoint Support.

Sample ControlPoint topology

This section provides an example of a distributed ControlPoint topology that adheres to the guideline of deploying SQL Server and the ControlPoint databases on a server that does not host any other ControlPoint components. This type of deployment provides optimal database performance.

NOTE: The following topology is intended as an example. Your ControlPoint environment might be different based on your size and scale requirements. For questions regarding sizing your environment, contact Micro Focus Support.

ControlPoint system topology



Size and scale considerations for IDOL content

NOTE: For more information on IDOL Content, see the *IDOL Explorer* and the *IDOL Getting Started Guide*, available from the [Micro Focus IDOL documentation site](#).

A major part of the design of an IDOL-based architecture depends on:

- How many documents you need to index into each instance of Content.
- How many Content servers that must run on each physical server, or equivalently, how many documents in total you need to index on each physical server.

If you know the total number of documents, the total number of physical servers required follows easily from these two points. However, in many cases you do not know the final number of documents, but instead need to scale the systems over time.

The upper limit on the number of documents for a server is likely to be determined by performance requirements. Multiple smaller servers tend to perform better than a single large one, because they can work in parallel on queries.

The key question is how many documents a server can index while remaining small. This value is tied to the local IDOL configuration, the type of data that you want to index, the type of queries that you will use, and the pattern of indexing and querying.

While you can derive very rough estimate figures by comparing with similar systems on similar hardware, the only reliable way to get useful statistics is to test your proposed system. That is, run an instance of ControlPoint and IDOL in the configuration you intend to use, on candidate hardware, and monitor performance while you index realistic data and send realistic queries.

When simulating load and assessing performance, you might also want to consider the following questions:

- Do you need query servers during indexing, or can you set up indexing to occur only during quiet times when query load is low (for example, overnight)?
- How many queries do you expect IDOL to handle simultaneously?

These statistics can give you a sensible maximum size for a single instance of Content, and also its likely system resource usage (footprint on disk, process memory size). After these values are known, you can determine the key values above.

Total disk usage by all Content servers on a machine cannot exceed the space available. Normal memory usage by all IDOL processes on a server ideally must fit in the machine's physical RAM, with enough free space remaining for the OS to effectively cache file system data.

Chapter 3: Install SQL Server

Before you install ControlPoint databases, you must install and configure SQL Server.

To install and configure SQL Server

1. [Install SQL Server software.](#)
2. [Configure SQL Server memory options.](#)

These options control the amount of memory that the SQL Server Memory Manager manages for a SQL Server process.

3. [Set the Windows power plan for the server.](#)

Changing the power plan provides SQL Server additional processing capacity.

Install SQL Server software

When installing SQL Server, adhere to the following guidelines:

- Use one of the supported versions of SQL Server, as listed in the *ControlPoint Support Matrix*. You can find this document on the [Micro Focus ControlPoint documentation site](#).
- Install SQL Server on a server dedicated to ControlPoint databases.

For optimal performance, install SQL Server on a server that will host only ControlPoint databases and no other ControlPoint components, such as connectors. Otherwise, to support other ControlPoint components on the same server, you must configure SQL Server to limit the resources it consumes.
- Ensure that SQL Server is accessible from the server that will host ControlPoint software.

To install SQL Server software

1. Install the SQL Server software, including Server Native Client.

For information about how to install the software, see the SQL Server documentation.

2. Apply the latest SQL Server service packs for your edition and version.

This included all currently-available and pushed SQL Server updates (critical updates and publicly-pushed individual updates) from Windows Update.

Configure SQL Server memory options

SQL Server Memory Manager uses two server memory options, **min server memory** and **max server memory** to manage the amount of memory allocated to a SQL Server process.

After installing SQL Server, set the maximum amount of server memory instead of using the default value. For example, reserve 1 GB of RAM for the OS, 1 GB for each 4 GB of RAM installed from 4 to 16 GB, and then 1 GB for every 8 GB RAM installed over 16 GB RAM.

For information about how SQL Server uses these options to allocate memory and the default value for each option, see your SQL Server documentation.

TIP: You can configure this memory option on either new or existing installations of ControlPoint.

Set the Windows power plan for the server

In Windows, the default power settings balance power efficiency and performance. For SQL Server to have consistent, predictable, and high performance, set the Windows power plan on the server to **High performance**. This additional processing capacity comes with higher power utilization.

TIP: You can set the power plan on either new or existing installations of ControlPoint.

To set the Windows power plan

1. Open **Control Panel > Power Option**.
2. Click **High performance**, and then click **OK**.

The server power options are set.

Chapter 4: Install ControlPoint databases

The first step in installing ControlPoint is to install and configure its databases.

To install and configure ControlPoint databases

1. Learn about the [ControlPoint databases](#) and their use of file groups.

ControlPoint has several databases, each supporting database partitioning and file groups that you must configure during installation.

2. [Prepare to install ControlPoint databases.](#)
3. [Configure the ControlPoint data source.](#)
4. [Install the ControlPoint databases.](#)
5. [Perform post-installation database tasks.](#)

After installing and configuring ControlPoint databases, you are ready to install ControlPoint IDOL and connectors.

TIP: The *ControlPoint Best Practices Guide*, available from the [Micro Focus ControlPoint documentation site](#), contains helpful information for working with ControlPoint databases.

ControlPoint databases

The ControlPoint environment contains the following databases:

- ControlPoint
- ControlPointAudit
- ControlPointExport (Optional)
- ControlPointMetaStore
- ControlPointMetaStoreTags
- ControlPointTracking

Database overview

ControlPoint supports SQL Server storage separation for multiple storage paths per database. This enables you to use more of the discrete, concurrent disk I/O available on your SQL Server host and can significantly increase performance.

Benefits of database partitions and file groups

Using database partitions and file groups provide the following benefits to all ControlPoint database implementations, regardless of size:

- Reduces the storage capacity required to operate the largest ControlPoint database, ControlPointMetaStore.

In addition, the storage structure of the databases is in smaller, more manageable files. This enables you to make use of smaller, more independent logical volumes.

- Reduces the storage throughput required for ControlPoint operations.

This reduction results from taking advantage of the concurrent storage channels/volumes usually available to production servers.

- Separates the structure of the database storage into multiple discrete files.

Having multiple files lets you more accurately monitor your server for I/O hotspots while under load and to easily relocate component files to additional volumes. It also allows you to preserve a standard logical internal structure and facilitates future upgrades, even if you performed custom reorganization of the storage files.

- Reduces SQL Server memory utilization.
- Adds SQL table and index partitioning.

This reduces the necessary SQL index maintenance windows and allows for more processing hours in a given day.

- Adds maintenance plans to all ControlPoint databases.

The maintenance plans can be tailored by database administrators as needed. These scheduled jobs, run by the native SQL Agent, intelligently perform rebuild, re-index, statistic calculation, and index compression tasks automatically and in an optimized fashion for both standard and partitioned objects, utilizing online index maintenance operations when available. For more information on SQL Server Agent jobs, see your SQL Server documentation.

By default, all of the new scheduled jobs run at 10 pm server time. If desired, you can adjust the nightly schedule times for each database. These start times may be staggered if desired, but it is important to ensure that the jobs are set to run at least once per day.

Logical file groups

The ControlPoint databases installation program prompts you for multiple paths per database, one for each logical file group defined in the database. These are then grouped by the three types of corresponding pages stored by SQL Server:

- Data
- Index
- Text (This covers both the now deprecated text and ntext SQL column data types, but also long char, nchar, varchar and nvarchar column types).

As the different databases that are used by ControlPoint are also segmented by schema, one file group per schema per type is available to be defined.

In each of the logical file groups, in the paths entered, multiple files will be placed in the target location in accordance with SQL Server best practices. For example, the number of files per file group equals the number of available processor cores up to a maximum of 16 per file group. After the database is created, the Database Administrator can move the individual files to any other storage target to further spread and control the SQL I/O utilization.

In addition, the installation program gives you the option to automatically *interleave* files from select file groups to multiple storage path targets. When this option is selected, paths that participate in the interleaving process are indicated in the database installer. Files from within each of these file groups will be spread evenly across all the participating paths.

File groups example

For the ControlPointMetaStore database on an 8 core SQL Server, when the interleave option is selected, causes two files from each of the Metadata.data, Metadata.index, MetaStore.data, and MetaStore.index file groups to be placed on each of their defined paths.

For small sized ControlPoint environments, or those without segmented performance disk storage attached, all file groups and their component files may be placed together in a single path.

However, to achieve optimal performance and scalability, particularly for large size databases, separation of storage to multiple paths, both by database and by file groups within each database, is strongly recommended.

Consult your systems architect for planning and guidance in this area, specific to your ControlPoint use and growth projections.

Prepare to install ControlPoint databases

Before you install the ControlPoint databases, there are a few tasks you must do to prepare your environment.

To prepare for ControlPoint databases

1. [Verify the SQL Server sa account.](#)
2. [Configure minimum SQL permissions.](#)
3. [Grant permissions on database file locations.](#)
4. [Start the SQL Server Agent service.](#)

Verify the SQL Server sa account

Ensure that the SQL Server **sa** account exists with its regular class of permissions and is not disabled.

This account will own the ControlPoint database maintenance jobs the installation process creates. If the account is removed, renamed, or disabled, the steps that create maintenance jobs will fail.

Configure minimum SQL permissions

Ensure the user account that deploys or upgrades the ControlPoint databases has permissions equivalent to the **sysadmin** default SQL login role, including the following permissions configured in SQL Server:

- **Dbcreator, public.** Required to create the ControlPoint databases.
- **SecurityAdmin.** Required to create users in the ControlPoint databases.

NOTE: Db_owner permissions are the minimum SQL permissions that can be used after the initial deployment.

Grant permissions on database file locations

Grant the appropriate read and write permissions on the directories you will configure for the database file groups. Permissions include standard permissions on the objects and UAC access (usually controlled by ownership inheritance), if applicable.

Follow these guidelines:

- **When utilizing a SQL user account.** Read and write access (and UAC access) granted to both the user account that runs the database installation program on the SQL server and the user account that operates the SQL Server instance.
- **When utilizing a Windows user account.** Read and write access (and UAC access) granted to the user account that runs the installation program.

These are the minimum permissions and access controls required for the directory targets. You can allow additional access to the directories if necessary.

Start the SQL Server Agent service

Ensure that the SQL Server Agent service is set for automatic start and that the service is running. The installation of the databases creates several SQL Server Agent maintenance jobs.

Configure the ControlPoint data source

Configure the ControlPoint data source in SQL Server Reporting Services (SSRS) to allow administrators to run ControlPoint reports from the ControlPoint Administration Console.

To configure the ControlPoint data source

1. Open **SQL Server Reporting Services Configuration Manager**.
2. Connect to the report server and instance.
3. On the Report Server Status page, verify that the Report Service is started.
4. Click the **Web Service URL** tab, where the virtual directory of the Report Server Web Service is defined.

Take note of the **Virtual Directory** name for later use during the configuration of the ControlPoint databases. In this example, the virtual directory name is **ReportServer**.

5. Click the **Report Manager URL** tab, where the URL to access Report Manager is defined.

Take note of the following information for use later during the configuration of the ControlPoint databases:

- **Virtual Directory**. In this example, the virtual directory name is **Reports**.
- **Report Manager URL**. In this example, the Report Manager URL is `http://<Localhost>:80/Reports`

6. Using a web browser, access the Report Manager URL.

The startup page of Report Manager appears. It contains the **Home** folder of the Report Manager.

7. Navigate to the **Micro Focus ControlPoint Reports > DataSource** folder.
8. Click the **ControlPointAudit** data source.

By default, the **Properties** tab of the ControlPointAudit data source appears.

9. Select one of the following connection options under the **Connect using** option:

Option	Description
Credentials supplied by the user running the report	User is prompted to specify credentials when the report is run.
Credentials stored securely in the report server	Credentials are used regardless of who requests a ControlPoint Audit report.
Windows integrated security	Every user who requests a ControlPoint Audit report must have an account in SQL Server with the Read permission to ControlPointMetaStore and ControlPoint Audit databases.
Credentials are not required	The configured unattended execution account is used. This must be an account in SQL Server with the Read permission to ControlPointMetaStore and ControlPoint Audit databases.

Install the ControlPoint databases

After configuring the ControlPoint data source, you are ready to install the ControlPoint databases.

TIP: The install process also installs SQL Agent jobs that automatically perform database maintenance suitable for most environments. However, you can configure these jobs to better support very large databases. For more information, see the information for advanced database maintenance controls in the *ControlPoint Administration Guide*. This document is available from the [Micro Focus ControlPoint documentation site](#).

Before you begin

Ensure the following:

- The SQL Server Agent service is set for automatic start and that the service is running.
- You have a plan for defining multiple file paths per database because you must specify those paths during the installation process.

For more information, see [Logical file groups, on page 19](#).

To install ControlPoint databases

1. Navigate to the \ControlPoint directory and run ControlPoint Database Installer.exe.

NOTE: If Windows UAC is enabled on the server, ensure that the user account running the installation program is also a user account in SQL Server that has sufficient permissions to update databases and sufficient permission to the database file locations.

The database installer opens to the Welcome page.

2. Click **Next**.

The Log Directory page opens.

3. Change the path of the setup log file, if necessary, and then click **Next**.

The SQL Connection page opens.

4. Enter the required **SQL Server** and **instance** names, or select them from the list.

5. Select the required authentication method: **Windows** or **SQL Server**.

If you select **SQL Server Authentication**, enter a **Login ID** and **Password**.

6. If only one disk is present, clear the **Enable interleaving for database transactions** option.

This option, selected by default, automatically interleaves files from select file groups to multiple storage path targets. Paths that participate in the interleaving process are indicated on each of the following Database Configuration pages.

Files from within each of these file groups will be spread evenly across all the participating paths.

7. Click **Test Connection** to verify the server details.
8. In the **Job Owner Username** field, enter a SQL Server user name for an account that has System Administrator access to SQL Server.

NOTE: The ControlPoint Database installation program uses this account to create and configure several SQL Server Agent maintenance jobs.

This user account must exist in SQL Server; the installation program does not verify it exists.

9. Click **Next**.
10. On each of the next several Database Configuration pages, perform the following steps:
 - a. Specify the path to the files listed, and then click **Next**.

You will configure database files for the following:

- ControlPoint database
- ControlPointAudit database
- ControlPointMetaStore database
- ControlPointMetaStoreTags database
- ControlPointTracking database

NOTE: When specifying data paths, keep the following in mind:

- If you selected the option to interleave database transaction interleaving in step 6, each page indicates the paths participating in the interleaving.
- Specify paths local to the server where SQL Server is installed.
- Place Index files on a different volume than the other components in the file group.
- Place Log files on a different volume than the other database files.

- b. On the ControlPoint Export Database Configuration page, to create a database to hold ControlPoint data for BI analysis, select the option listed.

For information about populating this database if you select this option, see the BI analysis information in the *ControlPoint Administration Guide* (available from the [Micro Focus ControlPoint documentation site](#)) or ControlPoint Help Center.

11. Click **Next**.

The ControlPoint Audit Reports page opens.
12. To upload audit reports to SQL Server Reporting Services (SSRS), select **Upload Reports** and click **Next**.

NOTE: This step requires that you configured a data source in SQL Server Reporting Services (SSRS). For more information, see [Configure the ControlPoint data source, on page 21](#).

If you select **Upload Reports**, the Reports Configuration page opens.

- a. In the **Audit Reports Installation** area, enter the installation path in the **Install reports to** field.
- b. In the Report Manager Server Settings area, enter the following information:
 - i. **Report Manager URL**
 - ii. **Report Manager Virtual Directory**
 - iii. **Report Webservice Virtual Directory**

NOTE: For **Report Manager Virtual Directory** and **Report Webservice Virtual Directory**, enter the values you previously defined on the SSRS Configuration Manager's **Report Manager URL** and **Web Service URL** tabs, respectively.

13. Click **Next**.
14. Verify the details on the Installation Confirmation page, and click **Install**.

The databases are installed.

IMPORTANT: Several SQL scripts are run as part of the database installation. If the scripts encounter problems during execution, the database installation program displays a dialog box prompting you to **Retry** or **Abort**.

If you choose **Abort**, the installation program attempts to drop the databases. If it cannot drop the databases, you will need to perform the following steps:

- a. In SQL Server Management Studio, ensure that there are no temporary tables in the **dbo.Temp_DBNames** path.

System databases > msdb > Tables > dbo.Temp_DBNames

- b. Manually drop the affected ControlPoint databases.
- c. Manually drop the **tempdb** database.

Dropping the databases avoids inconsistencies resulting from incomplete script executions.

- d. Restart the database installation program.

15. Review the installation log.
16. Either write down the hyperlinked connection string or click it to copy the string to your clipboard.

The ControlPointMetaStore service requires this connection string to access the **ControlPointMetaStore** database. You must save this connection string so you can use it

during the [Configure deployment packages, on page 29](#) task to configure the ControlPointMetaStore component's SQL connection string to the MetaStore database.

17. Click **Finish**.

The installation wizard closes.

Complete the ControlPoint installation process by [performing a few post-installation tasks](#).

Perform post-installation database tasks

After installing the ControlPoint databases, there are a few additional tasks to perform.

1. If you did not install the **ControlPointMetaStore** and **tempdb** databases on dedicated hard drives, move them so each is on its own dedicated hard drive.

For more information, see [Move the ControlPoint databases](#).

2. [Configure the recovery model for ControlPoint databases](#).

The default recovery model for all ControlPoint databases is **Simple**.

Move the ControlPoint databases

Due to high disk usage of the **ControlPointMetaStore** and **tempdb** databases, Micro Focus recommends that you allocate these databases their own dedicated hard drive.

For improved read and write performance of the **ControlPointMetaStore** database, Micro Focus also recommends the use of an enterprise-level solid-state drive (SSD).

NOTE: The following information illustrates how to move the **ControlPointMetaStore** and **tempdb** databases if they were not initially configured on dedicate hard drives.

The procedures are based on information provided in SQL Server documentation. For more information, see <https://docs.microsoft.com/en-us/sql/relational-databases/databases/move-user-databases?view=sql-server-2017>.

Example

This example describes how to move the **ControlPointMetaStore** and **tempdb** databases to dedicated hard drives E and F, respectively.

1. In SQL Server Management Console, run the following statement:

```
ALTER DATABASE ControlPointMetaStore SET OFFLINE;
```

IMPORTANT: The **tempdb** database cannot be set offline or online, so it is excluded from steps 1 and 4.

The database is set offline.

2. Move the file or files to the new location.

For example:

- Move ControlPointMetaStore.mdf to the E: volume
- Move tempdb.mdf to the F: volume.

3. For each file moved, run the following statement:

```
ALTER DATABASE ControlPointMetaStore MODIFY FILE ( name =  
ControlPointMetaStore_data, FILENAME =  
'E:\sqldata\ControlPointMetaStore.mdf' );
```

```
ALTER DATABASE tempdb MODIFY FILE ( name = tempdev, FILENAME =  
'F:\sqldata\tempdb.mdf' );
```

4. Run the following statement:

```
ALTER DATABASE ControlPointMetaStore SET ONLINE;
```

The database is set online.

5. Verify the file change by running the following query:

```
SELECT name, physical_name AS CurrentLocation, state_desc  
FROM sys.master_files  
WHERE database_id = DB_ID(N'ControlPointMetaStore');
```

```
SELECT name, physical_name AS CurrentLocation, state_desc  
FROM sys.master_files  
WHERE database_id = DB_ID(N'tempdb');
```

6. Stop and restart the instance of SQL Server for the change to take effect on **tempdb**.

Configure the recovery model for ControlPoint databases

The recovery model defines the type of transaction log the database maintains and therefore determines the restore options available should you need to restore the database. The default recovery model for all ControlPoint databases is automatically set to **Simple**. You can change the model to either **Full** or **Bulk-Logged** for each database to better meet your recovery needs.

To configure the recovery model

- For each ControlPoint, configure the recovery model using either SQL Server Management Studio or Transact-SQL.

For information about each type of recovery model and how to set one, see your SQL Server documentation.

Chapter 5: Install ControlPoint IDOL and connectors

This chapter describes how to install ControlPoint IDOL and connectors using deployment packages.

To install ControlPoint IDOL and connectors

1. [Create deployment packages](#) for the target servers.
2. Ensure your environment meets *all* requirements for ControlPoint IDOL, Metastore, and connectors, as listed in the *ControlPoint Support Matrix*. You can find this document on the [Micro Focus ControlPoint documentation site](#).

Requirements include software necessary for all connectors as well as software, user account provisioning, and license keys for specific connectors only. If you waited to install Microsoft Visual C++ Redistributable Packages and SQL Native Client from the deployment packages you created, be sure to install those components now.

3. [Install deployment packages](#) by copying them to them to the target servers, and then installing them.
4. (Optional) [Complete the Content Manager connector installation](#).
If you installed the Content Manager connector, finish its installation now.
5. (Optional) [Configure the Documentum connector](#).
If you installed the Documentum connector, configure it now.
6. (Optional) [Set up IDOL Content language types](#).
English is the only language provided by default.
7. [Start Windows services](#).

After installation, you can also do the following:

- [Deploy multiple MetaStore services](#)
- [Stop Windows services](#)
- [Uninstall deployment packages](#)

Create deployment packages

The ControlPoint IDOL Deploy Tool automates the creation of deployment packages for ControlPoint IDOL and connectors. This tool does not install the IDOL software directly; rather, it builds the deployment packages that you must copy to the target servers for subsequent installation.

To create deployment packages

1. [Configure deployment packages.](#)

The Deploy Tool configures the deployment packages, which require no further configuration for use with ControlPoint after the installation on target servers.

2. [Save deployment package configuration.](#)
3. [Build deployment packages.](#)

Configure deployment packages

Use the information in this section to run the Deploy Tool to configure deployment packages.

NOTE: You can run the Deploy Tool on any server to create ControlPoint IDOL deployment packages.

To configure deployment packages

1. Start the ControlPoint IDOL Deploy Tool by running `ControlPoint IDOL Deploy Tool.exe`.

The file is located in the `ControlPoint IDOL Deploy tool` directory.

The ControlPoint IDOL Deploy Tool is a self-extracting executable .

The Deploy Tool package build dialog box displays with four tabs: **General**, **IDOL**, **Connectors**, and **Components**.

2. On the **General** tab, enter the following information.

- **Deployment Mode.**
 - **Pilot.** Select **Pilot** to configure an IDOL system appropriate for a pilot or model office environment. The following defaults are used.
 - Log levels for all services are set to FULL.
 - The number of threads is reduced for applicable services for use on a small or shared server.
 - Memory usage is decreased for applicable services for use on a small or shared server.
 - The synchronization times for services are reduced so that analysis data is updated frequently.
 - **Production.** Select to configure an IDOL system appropriate for a production environment.
- **Advanced IDOL Distribution.** Choose whether to enable Advanced IDOL Distribution.

NOTE: Micro Focus recommends the Basic Distribution mode for most deployments. Advanced Distribution is beneficial only for very large environments. Using Advanced

Distribution mode requires additional planning, installation steps, and resources. We recommend that you contact support if you want to use Advanced Distribution mode.

Basic Distribution mode is no longer deprecated and ControlPoint 5.9.1 and later do not enable Advanced mode by default.

IMPORTANT: The use of Advanced IDOL Distribution results in underlying data changes that are irreversible. Once enabled and ControlPoint restarts, you cannot disable this feature.

- **Host Installation Directory.** Specify the directory for installing components on the target deployment servers.

The default location is: C:\Program Files\Micro Focus\ControlPoint\.

- **Host Package Build Location.** Specify the directory creating deployment packages when you run the Deploy Tool.

The default location is: C:\temp\ControlPoint\.

- **Zip File.** This option generates the deployment packages as compressed (ZIP) archives.

This option is useful when you plan to transfer deployment packages to different servers. The package size can exceed 1 GB.

- **Default Deployment Host.** Enter the name of the server that the ControlPoint IDOL Server software will be installed on.

NOTE: You will define the names of servers to host other components on the **Components** tab.

3. On the **IDOL** tab, enter the following information.

- **Number of IDOL Content Engines.** Enter the number of ControlPoint Content services to create.
- **Default Language Type.** Enter the default language type to be used by the ControlPoint IDOL Server.

The default language is **englishUTF8**.

- **Advanced IDOL Distribution.** If the **Advanced IDOL Distribution** check box on the **General** tab is selected, enter a name for the new IDOL database.

Make note of the name you use because you must specify the same name during a later configuration task. The default name is **ContentRepo**.

4. On the **Connectors** tab, select the connectors to deploy. Click **Config** to configure selected connectors, as follows:

- **File System Connector**
 - **Number of Connectors in Group.** Enter the number of connectors in the group. The maximum number is 9.

- **Deployment Hosts.** Enter the server names to which to deploy the connectors. Each server hosts one connector, however, if the number of specified servers is less than the number of connectors, the final server in the list hosts all remaining connectors.
- **Content Manager Connector**
 - **Number of Connectors in Group.** Enter the number of connectors in the group. The maximum number is 9.
 - **Deployment Hosts.** Enter the server names to which to deploy the connectors. Each server hosts one connector, however, if the number of specified servers is less than the number of connectors, the final server in the list hosts all remaining connectors.
- **SharePoint Remote Connector**
 - **Number of Connectors in Group.** Enter the number of connectors in the group. The maximum number is 9.
 - **Deployment Hosts.** Enter the server names to which to deploy the connectors. Each server hosts one connector, however, if the number of specified servers is less than the number of connectors, the final server in the list hosts all remaining connectors.
 - **SharePoint Credentials Username.** Enter the name of the user to use when authenticating with the SharePoint server.
 - **SharePoint Credentials Password.** Enter the password for the user to use when authenticating with the SharePoint server.
 - **SharePoint Credentials Domain.** Enter the domain of the specified user.
- **Exchange Connector**
 - **Number of Connectors in Group.** Enter the number of connectors in the group. The maximum number is 9.
 - **Deployment Hosts.** Enter the server names to which to deploy the connectors. Each server hosts one connector, however, if the number of specified servers is less than the number of connectors, the final server in the list hosts all remaining connectors.
 - **LDAP and Exchange Web Service User Domain.** Enter the user domain to use when connecting to both LDAP and the Exchange web service.
 - **LDAP and Exchange Web Service Username.** Enter the user name to use when connecting to both LDAP and the Exchange web service.
 - **LDAP and Exchange Web Service Password.** Enter the password to use when connecting to both LDAP and the Exchange web service.
- **Documentum Connector**
 - **Number of Connectors in Group.** Enter the number of connectors in the group. The maximum number is 9.
 - **Deployment Hosts.** Enter the server names to which to deploy the connectors. Each server hosts one connector, however, if the number of specified servers is less than the number of connectors, the final server in the list hosts all remaining connectors.
 - **Documentum Hosts.** Enter the name of the Documentum server.

- **Documentum Credentials Username.** Enter the name of the user to use when authenticating with the Documentum server.
- **Documentum Credentials Password.** Enter the password for the user to use when authenticating with the Documentum server.

NOTE: All information entered related to Documentum Connector are case-sensitive.

- **Hadoop Connector**

- **Number of Connectors in Group.** Enter the number of connectors in the group. The maximum number is 9.
- **Deployment Hosts.** Enter the server names to which to deploy the connectors. Each server hosts one connector, however, if the number of specified servers is less than the number of connectors, the final server in the list hosts all remaining connectors.
- **Hadoop Root URI.** Enter the root URI of the file system to which to connect.
- **Hadoop Path.** Enter the path in the file system to process for files.

- **Notes Connector**

- **Number of Connectors in Group.** Enter the number of connectors in the group. The maximum number is 9.
- **Deployment Hosts.** Enter the server names to which to deploy the connectors. Each server hosts one connector, however, if the number of specified servers is less than the number of connectors, the final server in the list hosts all remaining connectors.

5. On the **Components** tab, click **Config** next to a component name to configure that component.

You can configure the following items for each component.

- **Host.** The name of the server to which to deploy this component.
- **Path.** The installation location for this component.

6. For the **ControlPointMetaStore** component, specify the SQL connection string to use when connecting to the MetaStore database.

Enter the connection string you previously saved or copied to clipboard during the [Install ControlPoint databases](#) task. Make any required adjustments.

The connection string has the following general format when ControlPoint databases are configured to use Windows authentication:

```
Driver={SQL Server Native Client 11.0};App=ControlPoint;Server=
servername;Database=ControlPointMetaStore;Trusted_Connection=yes
```

Alternatively, to specify a connection to a specific named SQL instance instead of the default one, use the following format:

```
Driver={SQL Server Native Client 11.0};App=ControlPoint;Server=
servername\instancename;Database=ControlPointMetaStore;Trusted_Connection=yes
```

Save deployment package configuration

After configuring your deployment packages, save the settings to a file.

To save all configuration settings:

- Select **Save** or **Save As** from the Deploy Tool's File menu.

Build deployment packages

The last step in the process of creating deployment packages is to build them.

To build deployment packages

- Click **Deploy**, or select **Deploy** from the Deploy Tool's Actions menu.

The tool creates the packages as either directories or .ZIP files (if you selected the **Zip File** option) in the location you specified for the **Host Package Build Location** option. The default location is: C:\temp\ControlPoint\.

Install deployment packages

After using the Deploy Tool to create deployment packages, use the information in this section to install them.

Before you begin

Do the following:

- Ensure that your environment meets all requirements for ControlPoint IDOL and connectors, as listed in the *ControlPoint Support Matrix*.

You can find this document on the [Micro Focus ControlPoint documentation site](#). Requirements include software, account provisioning, and IDOL license keys.

- Move the deployment packages to each target server so they are available for installation.

The Deploy Tool creates the packages as either directories or .ZIP files in the location you specified for the **Host Package Build Location** option.

To install a deployment package

1. As the local administrator, run the `_deploy_services.bat` Windows batch file.

The batch script copies the components to the location defined in **Host Installation Directory**.

NOTE: If Windows UAC is enabled on the server, you must run the batch file manually from the command line.

- a. Open a command prompt as an Administrator.
- b. Change the directory to the temporary location that contains the batch file.
- c. Run `_deploy_services.bat`.

2. As the local administrator, run the `_install_services.bat` file to install the Windows services.
3. When prompted, enter the credentials for the first connector in the deployment package.

Enter the credentials in the following format.

Please enter username: *domain\username*

Please enter password: *password*

Ensure that you include the domain or host name when entering the user name.

4. When prompted, decide whether to use the same credentials for all other connectors.
If you use different credentials for other connectors, enter them in the same format.

5. When prompted, enter the credentials to use for your ControlPointMetaStore service.

Enter the required user name and password.

6. Copy the IDOL license file to the IDOL License Server directory after installation but before services start.

Rename the IDOL license key to `licensekey.dat` and place it into the `LicenseServer` directory at the following location:

`Program Files\Micro Focus\ControlPoint\LicenseServer`

Complete the Content Manager connector installation

If you deployed the Content Manager connector, you must complete its installation before using it.

To complete the Content Manager connector installation

- Copy the following files from the Content Manager client installation folder (Program Files\Micro Focus\Content Manager, by default) to the Program Files\Micro Focus\ControlPoint\Indexer\Content Manager Connector folder:
 - `HP.HPTRIM.SDK.dll`
 - `HP.HPTRIM.SDK.xml`

Configure the Documentum connector

If you deployed the Documentum connector, there are a few additional configurations to perform before using it.

Before you begin

Ensure you have the set of .Jar files that the Documentum connector requires. This task requires you to copy them into a specific folder.

NOTE: ControlPoint does not provide these files. For information or help obtaining these files, contact the Documentum Support team.

To configure the Documentum connector

1. In a text editor, update the `Program Files\Micro Focus\ControlPoint\Indexer\Documentum Connector\dfc.properties` file to include your Documentum server's host and port:

```
dfc.docbroker.host[0]=DocumentumHostName  
dfc.docbroker.port[0]=DocumentumPort
```

2. Copy the `dfc.properties` and `dfc.keystore` files from:

`Program Files\Micro Focus\ControlPoint\Indexer\Documentum Connector`

to the following two locations:

- `Program Files\Micro Focus\ControlPoint\Indexer\OGS`
- `Program Files\Micro Focus\ControlPoint\Commons\dfc`

3. Add the .Jar files required by the Documentum connector to the `Program Files\Micro Focus\ControlPoint\Commons\dfc` folder.

Set up IDOL Content language types

By default, the IDOL Content configuration file contains only an entry for English in the `[LanguageTypes]` section. If you need to support other languages, identify those languages and update the Content configuration file accordingly. For more information, see the IDOL documentation or contact Support.

Start Windows services

You can start all Windows services on a host or only services for a specific component.

To start all Windows services

- As the local administrator, run `_start_services.bat`, located in `\temp\ControlPoint\host_hostName`.

To start Windows services for a specific component

- As the local administrator, run `_start_service.bat`, located in the component-specific `\temp\ControlPoint\host_hostName\component` folder.

NOTE: If IDOL content engines are on a different server than the IDOL connectors, Micro Focus recommends that you start and verify the IDOL services before the connectors start.

Starting the connectors starts the analysis process for the locations specified when configuring connectors in the Deploy Tool.

Stop Windows services

You can stop all Windows services on a host or only services for a specific component.

To stop all Windows services

- As the local administrator, run `_stop_services.bat`, located in `\temp\ControlPoint\host_hostName`.

To stop Windows services for a specific component

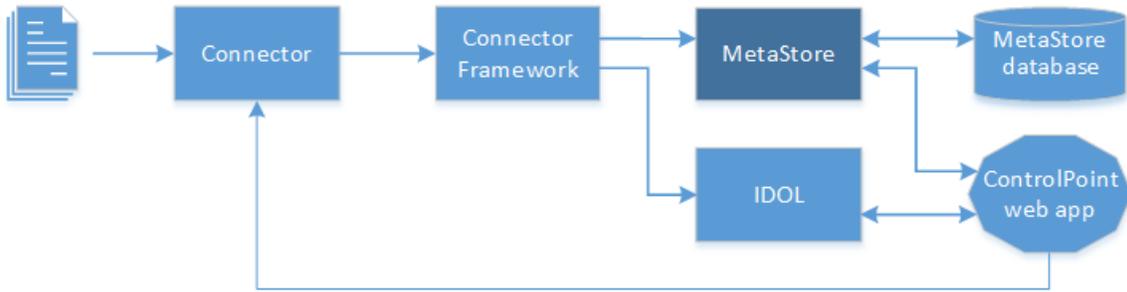
- As the local administrator, run `_stop_service.bat`, located in the component-specific `\temp\ControlPoint\host_hostName\component` folder.

Deploy multiple MetaStore services

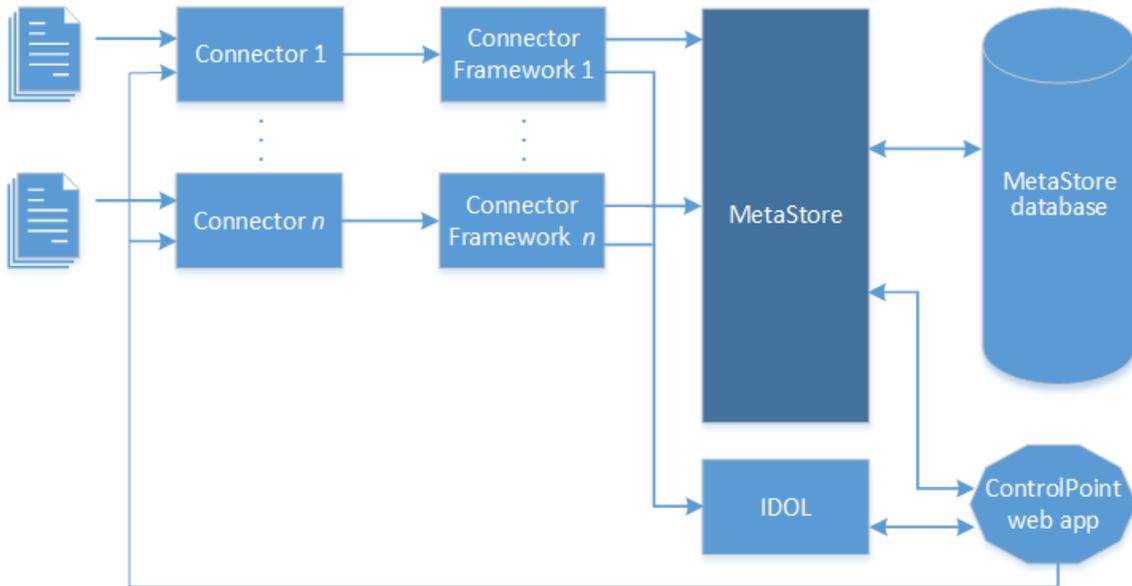
The default ControlPoint deployment contains a single MetaStore service node. However, if you add multiple connectors to your deployment to ingest different types of documents, deploying additional MetaStore nodes will improve performance.

Overview

The ControlPoint installation process deploys a single MetaStore service node. This node ingests data from the Connector Framework and communicates with the MetaStore database (to store data) and the ControlPoint web application (to get user-created rules and policies for document management). The following figure illustrates the data flow in the default deployment.

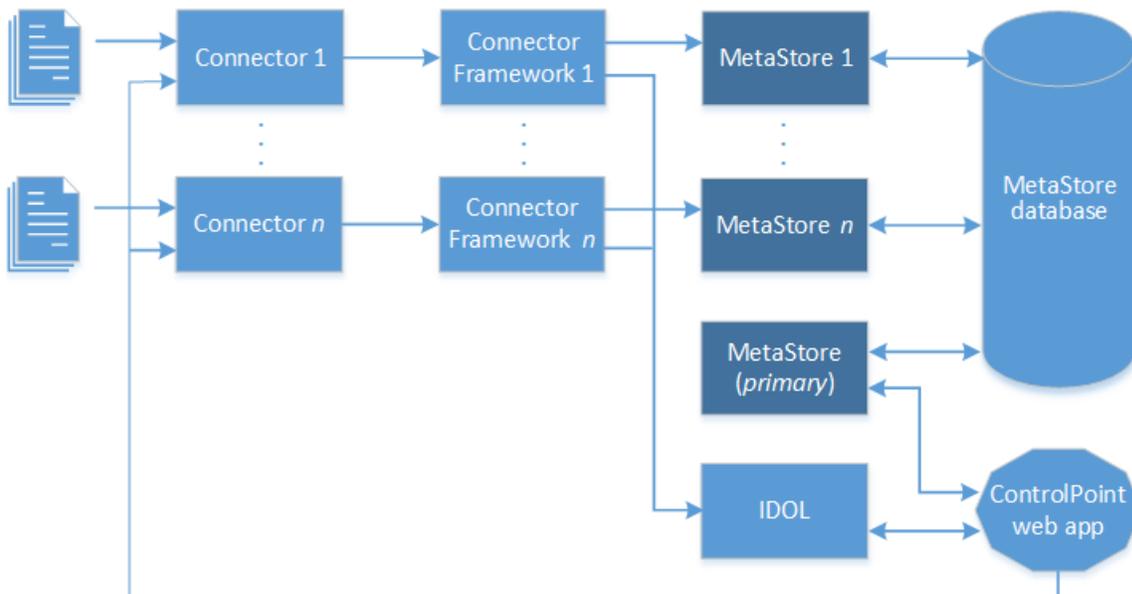


To support a variety of document types, you can add additional connectors that each feed the single MetaStore, as shown.



However, as the system grows, the MetaStore becomes a bottleneck as it tries to process data from all connectors in addition to interacting with data from the web application.

To prevent this issue and enhance the system's document ingestion performance, you can deploy additional MetaStore service nodes so that there is a 1-to-1 relationship between connectors and MetaStore components. In this type of deployment, the original MetaStore node remains and serves as the primary. It is dedicated to control the operations users perform through the ControlPoint web application, such as creating, updating, and deleting policies or repositories. The additional MetaStore nodes handle ingestion of documents and policy execution.



NOTE: There is no direct communication between the primary MetaStore node and IDOL. Instead, both components provide the web application with information needed by the tasks the user performs. In return, the web application sends them component-specific instructions to carry out in order to help fulfill the user's chosen task.

The following sections explain how to the deploy additional MetaStore nodes into your ControlPoint environment. You should deploy these nodes only after you deploying all other connectors and IDOL components.

Prepare for deployment

1. Decide whether the additional MetaStore service node will reside on the same server as the other IDOL engines, or on a separate server.

NOTE: Micro Focus recommends that you deploy the additional MetaStore component on same machine as the Connectors performing the ingestion actions.

2. If needed, install the SQL Server Native Client software to the MetaStore host. For more information, see your SQL Server documentation.
3. The MetaStore component requires two unused port during configuration.

Verify the unused ports by running the following command:

```
netstat -anob | findstr "4500"
```

If the ports are already used, select two different ones and verify that they are unused.

Deploy the additional MetaStore component

To deploy multiple MetaStore components

1. Stop the MetaStore service.
2. Copy the MetaStore folder to a new location.

For example:

```
Copy Program Files\Micro Focus\ControlPoint\Indexer\MetaStore to  
<newPath>\MetaStore2
```

where

<newPath> is the new path for MetaStore2.

TIP: If you are copying the MetaStore folder to another server, Micro Focus recommends that you still rename the folder and components to MetaStore2, in order to uniquely identify the additional components.

3. Navigate to the MetaStore2 folder and rename the files as follows:
 - ControlPoint MetaStore.exe to ControlPoint MetaStore2.exe
 - ControlPoint MetaStore.cfg to ControlPoint MetaStore2.cfg
4. Open ControlPoint MetaStore2.cfg in a text editor and edit the following settings:
 - a. In the [Server] section, change the port number to an unused port number.
 - b. In the [Service] section, change the port number to another unused port number.
5. Save the file.

Modify the Install and Uninstall MetaStore scripts

The scripts for installing and uninstalling IDOL components must be modified to include the additional MetaStore component.

1. On the server hosting the MetaStore2 component, navigate to the MetaStore2 folder.

For example:

```
Program Files\Micro Focus\ControlPoint\Indexer\MetaStore2.
```

2. Open install_metastore.bat in a text editor.
3. Update the following path to reference the path to MetaStore2:

```
pushd "E:\Program Files\Micro Focus\ControlPoint\Indexer\Metastore2"
```

4. Open `uninstall_metastore.bat` in a text editor.
5. Update the following path to reference the path to `MetaStore2`:

For example:

```
pushd "E:\Program Files\Micro Focus\ControlPoint\Indexer\Metastore2"
```

6. Save the file.

Modify the Install Services script

1. Open the `_install_service.bat` in a text editor.
2. Update the following paths to reference the path to `MetaStore2`.

For example:

```
echo y| cacls "E:\Program Files\Micro Focus\ControlPoint\Indexer\Metastore2" /E  
/T /G %wsmssvcun:~2%:F
```

```
echo y| cacls "E:\Program Files\Micro Focus\ControlPoint\Indexer\Metastore2" /E  
/T /G %wsmssvcun%:F
```

3. Update all service names from `Metastore` to `MetaStore2`:

```
"ControlPoint MetaStore2.exe" -install
```

```
sc config "ControlPoint MetaStore2" obj= "%wsmssvcun%" password= "%wsmssvcpw%"
```

```
sc failure "ControlPoint MetaStore2" reset= 0 actions= restart/60000
```

4. Save the file.

Modify the Start Services script

1. Navigate to the `MetaStore2` folder.

For example:

```
Program Files\Micro Focus\ControlPoint\Indexer\MetaStore2.
```

2. Open `_start_service.bat` in a text editor.
3. Update all service names from `Metastore` to `MetaStore2`:

```
net start "ControlPoint MetaStore2"
```

4. Save the file.

Modify the Stop Services script

1. Open `_stop_service.bat` in a text editor.
2. Update the URLs with the host name and new port number.

```
http://hostname:4512/action=stop
```

Where:

- **hostname** is the MetaStore server
- **4512** is the new port number

3. Save the file.

Associate Connector Framework Services (CFS) to the new MetaStore component

To complete the configuration of multiple MetaStore components, you must update the Connector Framework Services to use the new MetaStore component.

1. On the Connector, open the CFS configuration file.

For example, for a FileSystem connector, open the `ControlPoint FileSystem Connector Framework.cfg` located in the following location:

```
\Program Files\Micro Focus\ControlPoint\Indexer\FileSystem Connector Framework
```

2. Update the `[MyMetaStoreIndex]` section to reference the new MetaStore. In this example, it is MetaStore.

```
[MyMetaStoreIndex]  
Type=MetaStore  
Host=hostname  
Port=4512
```

3. On the MetaStore servers, start the MetaStore services.

Uninstall deployment packages

To upgrade or remove IDOL or specific components, uninstall the appropriate deployment packages.

To uninstall all components

- As the local administrator, run the `_uninstall_services.bat` script, located in `\temp\ControlPoint\host_<hostName>`.

To uninstall a specific component

- As the local administrator, run `_uninstall_service.bat`, located in the component-specific `\temp\ControlPoint\host_hostName\component` folder.

Chapter 6: Install ControlPoint components

This chapter describes process of installing ControlPoint components.

To install ControlPoint components

1. Ensure your environment meets *all* software requirements for ControlPoint, as listed in the *ControlPoint Support Matrix*. You can find this document on the [Micro Focus ControlPoint documentation site](#).

Requirements include Microsoft Visual C++ Redistributable Packages and SQL Native Client. If you waited to install these components from the ControlPoint IDOL and connectors deployment packages you created, be sure to install them now.

2. [Enable Federal Information Processing Standards \(FIPS\) security mode](#).
3. [Install ControlPoint and the ControlPoint Engine](#).
4. [Configure ControlPoint](#).
5. If you enabled ControlPoint security, update ControlPoint configuration files as described in [Configure ControlPoint security settings](#).

After installation, you can also perform the following optional task:

- [Deploy ControlPoint by enabling HTTPS](#)

Enable Federal Information Processing Standards (FIPS) security mode

The Federal Information Processing Standard (FIPS) is a United States government standard that specifies best practices for implementing cryptographic algorithms, handling key material and data buffers, and working with the operating system. ControlPoint uses the SHA-1 encryption algorithm in a FIPS-compliant library.

NOTE: If you do not plan to use FIPS in your ControlPoint environment, ignore this section and proceed to [Install ControlPoint and the ControlPoint Engine](#).

Limitations

ControlPoint has the following limitations when interacting with FIPS:

- ControlPoint does not support changing the FIPS security mode after ControlPoint has been deployed to the environment. After the selection has been made in Configuration Manager, it cannot be changed by redeploying ControlPoint.
- The Remote Analysis Agent (RAA) utility does not support running with the FIPS security mode.

Enable FIPS

To install ControlPoint on FIPS-enabled Windows servers, you must enable FIPS on the servers before you install and deploy ControlPoint.

To enable FIPS

- Follow the steps that your Windows documentation provides for enabling FIPS encryption.

After installing ControlPoint, you will enable FIPS in your ControlPoint environment when configuring ControlPoint using Configuration Manager.

Install ControlPoint and the ControlPoint Engine

This section describes how to install ControlPoint and the ControlPoint Engine.

Before you begin

Ensure that the server you plan to install the software on meets all ControlPoint requirements listed in the *ControlPoint Support Matrix*. You can find this document on the [Micro Focus ControlPoint documentation site](#).

To install ControlPoint Console and Engine

1. Run `setup.exe` as the Administrator.
The file is located in the `ControlPoint\` directory.
The Welcome page opens.
2. Click **Next**.
The License Agreement page opens.
3. Select **I accept the terms** in the license agreement, and then click **Next**.

The Customer Information dialog box appears.

4. Enter your User Name and Organization, and then click **Next**.

The Setup Type page opens.

5. Select the setup type that meets your requirements.
 - **Typical** installs ControlPoint and the ControlPoint Engine.
 - **Complete** installs ControlPoint, Engine, and Web Services.
 - **Custom** allows the selection of individual components, as required.
6. Click **Next**.

The Destination Folder dialog box appears.

7. (Optional) Click **Change** to change the default installation location.
8. Click **Next**.
9. Review the installation settings that you provided, and then click **Install**.
10. Click **Finish** to exit the installer.

If you select **Launch ControlPoint Configuration Manager**, the Configuration Manager starts.

Configure ControlPoint

You can configure the ControlPoint system centrally using ControlPoint Configuration Manager.

NOTE: This task assumes that you are configuring the Content Manager environment on one server.

Before you begin

Ensure the following two items:

- The user account you will use to run Configuration Manager is also a SQL Server user that has permissions equivalent to the **sysadmin** default SQL login role, including the following permissions configured in SQL Server:
 - **Dbcreator, public.** Required to create the ControlPoint databases.
 - **SecurityAdmin.** Required to create users in the ControlPoint databases.
- Ensure that you have Windows Authentication installed through Windows Server Manager.

To configure ControlPoint

1. Launch ControlPoint Configuration Manager.

You can launch the Configuration Manager from the ControlPoint program group.

NOTE: Settings in Configuration Manager are grouped by configuration area. Use the left panel navigation tabs to configure each group of settings.

You must complete all mandatory settings before you can deploy the ControlPoint components by clicking **Deploy**.

2. Enter the **SQL Server** and **instance**, or select it from the list.
3. Specify the connection method: **Windows Authentication** or **SQL Server Authentication**.
If you select **SQL Server Authentication**, enter a Login ID and a Password.
4. Click **Connect**.

The ControlPoint Configuration Manager opens to the **Database Settings** tab.

5. The **Database Settings** tab displays the connection settings entered during the database installation.

NOTE: If you use **SQL Server Authentication**, you can provide alternate login and password credentials. The login credentials must exist in SQL Server.

6. On the **IIS Settings** tab, specify the following settings:
 - a. Specify the website to deploy the ControlPoint web applications to.

NOTE: The deployed web applications can subsequently be retracted by selecting **Not Deployed** from the list.

- b. Specify the **User Account settings** for the IIS Application Pool to use. Each of the ControlPoint web applications use the IIS Application Pool.

Enter the **Domain**, **Username** and **Password** in the appropriate boxes.

NOTE: The specified user must be a member of the **Allow log on Locally** policy, which you can set in the Windows Local Security Policy console through the following path: **Security Settings > Local Policies > User Rights Assignments > Allow log on locally**.

7. On the **Engine** tab, specify the following settings:
 - a. To update the account used as the identity for the ControlPoint Engine service, select **Update Engine Service Account**, and then enter the appropriate account information.

NOTE: The Engine Service account identity will be used for user impersonations in ControlPoint, regardless of the account set for the Application Pool.

- b. Enter the number of threads for the Engine to use.

NOTE: Micro Focus recommends that the number of threads to be the number of processors in the ControlPoint Engine server.

- c. Policy execution requires a temporary location that is accessible by all ControlPoint connectors. The Configuration Manager can create and use a default network share named **ControlPointTempLocation** on the local server or you can chose an alternate network share that you created.
8. On the **Data Analysis** settings tab, specify the following settings:
 - a. Select **Make this system the active Data Analysis Controller**.

This setting determines whether the current system should be the active Data Analysis Controller or not.

The SQL server name is the **Data Analysis Controller Host**.
 - b. Enter a port number in the **Data Analysis Controller Port** box.
 - c. In the IDOL Statistics Server Settings section, specify the **Statistics Host, Port, and Index Port** for the statistics server.
 9. On the **IDOL** settings tab, enter the settings:
 - a. Enter the **DIH Host, Port, and Index Port** numbers.
 - b. Enter the **Distributed Connector Host** and its **Port** number.
 - c. Enter the **DAH Host** name and **Port** number your Micro Focus IDOL DAH component.
 - d. Enter the name of the **Agent Store Host, Port, and Index Port** numbers.
 - e. Enter the **Category Host** name and its **Port** number.
 - f. Enter the **Community Host** name and its **Port** number.
 - g. Enter the **View Host** and its **Port** number.
 - h. Enter the name of the **OGS Host** and its **Port** number.
 - i. Configure use of the Advanced IDOL Distribution feature.

IMPORTANT: The use of Advanced IDOL Distribution results in underlying data changes that are irreversible. If you are upgrading an installation that has Advanced IDOL Distribution enabled, you cannot disable it.

- To use Basic Distribution (recommended for most deployments), clear the **Enable Advanced IDOL Distribution** check box.
- To use Advanced Distribution (recommended only for very large environments), do one of the following:
 - If installing ControlPoint or upgrading from a previous version that already has this feature enabled:
 - i. Ensure the **Enable Advanced IDOL Distribution** check box is selected.
 - ii. Enter the name of the IDOL database name that you specified on the **IDOL** tab of the IDOL Deploy Tool while configuring the deployment packages during ControlPoint installation.

For example: ContentRepo (default value)

- If upgrading ControlPoint from a version that is not already configured for this feature:
 - Clear the **Enable Advanced IDOL Distribution** check box.

A post-upgrade task, which involves more than just selecting this option, covers the complete process of how to enable it.
 - j. To enable IDOL OEM licensing, select the **Enable OEM License** check box, and then in the **IDOL OEM Encryption Key** field, enter the key that you received with the IDOL LicenseKey.dat file.
 - k. In the MetaStore Service Settings section, enter the **MetaStore Host** name and **Port** number.
 - l. To specify a custom location for Insert Configurations, under **Target Location Insert Settings**, clear the **Use Local Configuration** check box. Then, in the **Insert Configuration Location** field, enter the shared network location to use.
 - m. In the **Date Format** list, select the date format ControlPoint uses.

The default format is: mm/d/yy
10. On the **Security** settings tab, specify options for enabling security:

- To enable ControlPoint security, select **Enable Security**.

If enabled, specify the ControlPoint system administrator account, the Active Directory server, and a distinguished name.

You will complete the process of enabling security during the post-install step [Configure ControlPoint security settings](#).

NOTE: If enabling ControlPoint security, you must disable ASP.NET Impersonation in Internet Information Server (IIS).

In IIS, go to **Sites > Default Web Site > Click ControlPoint > Authentication >** and ensure that **ASP.NET Impersonation** is disabled.

- To enable Federal Information Processing Standards (FIPS) security mode, select **Enable FIPS**.

IMPORTANT: This setting configures FIPS for environments that contain a single MetaStore database residing on the ControlPoint server. However, if you install the MetaStore database on a different server or install multiple MetaStore databases, you must manually enable FIPS by configuring the following Windows environmental variable on all servers that host a MetaStore database:

- **Name:** ENABLEFIPS
- **Value:** True

NOTE: The following are other FIPS-related items to take into consideration:

- If you enable FIPS as the security mode and the ControlPoint environment is deployed, you cannot change the FIPS security mode. For more information, see [Enable Federal Information Processing Standards \(FIPS\) security mode](#).
- When FIPS security is used in combination with the **Make this system the active Data Analysis Controller** option on the **Data Analysis** tab, the active controller is the master, and FIPS security works seamlessly.

If the **Make this system the active Data Analysis Controller** option is cleared, this server acts as a subordinate node. The host name of a master controller is extracted from the database and displayed in Configuration Manager and the **Enable FIPS** option is disabled.

11. On the **Mail Server** settings tab, specify the following settings to enable email notifications.

- **Mail Server settings**

- **Server.** Enter the server name of an SMTP mail server. For example, `mySMTPserver.mycompany.com`
- **From.** Enter an email address from which messages will be sent. For example, `myAdmin@mycompany.com`.

The settings are used for the Notify Policy Approvers scheduled task. The scheduled task sends out email notifications for policies configured for Review before execution. For more information on scheduled tasks, see the *ControlPoint Administration Guide* (available from the [Micro Focus ControlPoint documentation site](#)) or the ControlPoint Help Center.

- **SMTP client connection settings**

- **Port.** Enter the port number on which your SMTP server listens for connections.
- **Enable SSL.** If your SMTP server is configured for SSL, ensure this check box is selected. Otherwise, clear this option. This option is selected by default.

12. On the **WebAPI** settings tab, configure the following options:

- **Swagger Theme:** Select a theme for the Swagger UI that provides access to the ControlPoint API.
- **Web API Version:** Select which version of the ControlPoint API the Swagger UI uses by default.

TIP: You can also change the API version from within the Swagger UI. To do so, in the UI header, select the URL for the version you want to use, and then click **Explore**.

- **Authentication Token Endpoint:** This read-only field specifies `/api/login` as the authentication token endpoint.
- **Token Duration (minutes):** Specify the number of minutes that the API-generated authentication token remains valid. The default is 60.

For information about accessing the ControlPoint API, see either the *ControlPoint Administration Guide*, available from the [Micro Focus ControlPoint documentation site](#), or the ControlPoint Help Center.

13. Click **Deploy**.

The ControlPoint components are deployed.

NOTE: If you uninstall and reinstall the ControlPoint software for any reason, the Add/Remove Programs dialog displays an option to retain or remove the FIPS security mode. Click **Yes** to retain the FIPS security mode, or **No** to remove it.

Deploy ControlPoint by enabling HTTPS

This section provides the information required to deploy ControlPoint by enabling HTTPS in the environment.

1. [Enable HTTPS](#).
2. [Redeploy ControlPoint when HTTPS is enabled](#).
3. [Configure the Redirector service for HTTPS](#).

Enable HTTPS

To enable HTTPS in the environment, you must perform the following tasks.

1. [Create certificates](#) to sign the server and client certificates.
These certificates must be added to the certificate stores.
2. [Configure certificate usage in IIS Manager](#).
3. [Update ControlPoint component configuration files](#).

Create certificates

Create a certificate authority to sign the server and client certificates. The server certificate is required for authentication. The client certificate is optional.

NOTE: When generating the certificates, do not use the SHA-1 algorithm as it has been deprecated.

To create the certificates

1. Import the pfx file for the Certificate Authority to the Local Computer's Trusted Root Certification Authorities.
2. Import the pfx file for the Server certificate to the Local Computer's Personal certificate store.

3. (Optional) Import the pfx file for the Client certificate to the Current User Personal certificate store and into the browser's certificate store.

Configure certificate usage in IIS Manager

Import the certificates to IIS Manager and configure bindings and application settings.

To import certificates to IIS

1. In the IIS Manager, from the navigation pane on the left, select the server and select the Server Certificates.
2. Select **Import** and locate the .pfx file. This is the Personal Information Exchange file generated as part of the certificate making process.
3. Enter the file **Password**.

To configure the bindings

1. In the IIS Manager, from the navigation pane on the left, select the website.
2. In the right pane, from Edit Site, select **Bindings**.
3. Click **Add** and in the Edit Site Binding window, set **Type** to HTTPS.
4. Enter the host name.
5. Select **Require Server Name Indication** and select your certificate.
6. Click **OK**.

To configure IIS to require certificates

Configure the ControlPoint, DataAnalysisService and CPWS apps in IIS Manager to require certificates.

ControlPoint app

1. Click **SSL Settings**.
2. Select **Require SSL**.
3. Under **Client Certificates**, select **Accept**.

To disable client certificate popup when accessing the ControlPoint from browser

1. Go to **IIS**.
2. In IIS, go to **Sites** > select **ControlPoint** > Double click on **SSL Settings** from the middle pane.
3. Under **Client Certificates**, select **Ignore**.

Data AnalysisService app

1. Click **SSL Settings**.
2. Select **Require SSL**.
3. Under **Client Certificates**, select **Accept**.

CPWS app

1. Click **SSL Settings**.
2. Select **Require SSL**.
3. Under **Client Certificates**, select either **Ignore** or **Accept**.

Update ControlPoint component configuration files

Configure the ControlPoint Administration Console to communicate with the Dashboard and Data Analysis Services using HTTPS and to require user authentication.

To update the Dashboard: Web.config file

1. Navigate to: \Program Files\Micro Focus\ControlPoint\Dashboard\Web.config in the production environment.
2. Comment out the `system.serviceModel` tag located below the `Begin HTTP Service Model` comment.
3. Uncomment the `system.serviceModel` tag located below the `Begin HTTPS Service Model` with `certificate` comment.

There are two similar tags so be sure to uncomment the certificate-related one.

4. In the two endpoint tags, replace the address's value of `localhost` with the host name of your environment. For example, `server1.XYZCorp.com`.
5. In the `clientCertificate` tag, do the following:
 - If you did *not* import the `pfx` file for the Client certificate to the Current User Personal certificate store when creating the certificates, change the value of `storeLocation` from `CurrentUser` to `LocalMachine`.
 - Change `findValue` to be the thumbprint of your client certificate.

Locate your client certificate thumbprint by opening your client certificate and navigating to the details.

TIP: Other methods of finding the certificate can also be used. For more information, see [https://msdn.microsoft.com/en-us/library/ms731323\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/ms731323(v=vs.110).aspx)

CAUTION: When entering the thumbprint:

- Enter the value manually by typing it into the file.
Do not copy and paste this value from the certificate because the encoding adds hidden characters that will cause issues.
- Do not include whitespace in the thumbprint value you enter.
For example, if the thumbprint from the certificate begins with: **a1 b2 c3 d4 e5...**
Enter: **a1b2c3d4e5...**

To update the DataAnalysis Service: Web.config file

1. Navigate to: \Program Files\Micro Focus\ControlPoint\DataAnalysis\Service\Web.config in the production environment.
2. Comment out the `system.serviceModel` tag located below the `Begin HTTP Service Model` comment.
3. Uncomment the `system.serviceModel` tag located below the `Begin HTTPS Service Model` with `certificate` comment.

There are two similar tags so be sure to uncomment the certificate-related one.

To update ControlPoint Timer: app.config file

1. Navigate to: \Program Files\Micro Focus\ControlPoint\Engine\Scheduler\ControlPointTimer.exe.config in the production environment.
2. Comment out the `system.serviceModel` tag located below the `Begin HTTP Service Model` comment.
3. Uncomment the `system.serviceModel` tag located below the `Begin HTTPS Service Model` with `certificate` comment.

There are two similar tags so be sure to uncomment the certificate-related one.

4. In the two endpoint tags, replace the address's value of `localhost` with the host name of your environment. For example, `server1.XYZCorp.com`.
5. In the `clientCertificate` tag, do the following:
 - If you did *not* import the `pfx` file for the Client certificate to the Current User Personal certificate store when creating the certificates, change the value of `storeLocation` from `CurrentUser` to `LocalMachine`.
 - Change `findValue` to be the thumbprint of your client certificate.

To update WebService: Web.config file

1. Navigate to: \Program Files\Micro Focus\ControlPoint\WebService\Web.config in the production environment.

2. Comment out the `system.serviceModel` tag located below the `Begin HTTP Service Model` comment.
3. Uncomment the `system.serviceModel` tag located below the `Begin HTTPS Service Model` with `certificate` comment.

There are two similar tags so be sure to uncomment the certificate-related one.

4. In the two endpoint tags, replace the address's value of `localhost` with the host name of your environment. For example, `server1.XYZCorp.com`.
5. In the `clientCertificate` tag, do the following:
 - If you did *not* import the `pfx` file for the Client certificate to the Current User Personal certificate store when creating the certificates, change the value of `storeLocation` from `CurrentUser` to `LocalMachine`.
 - Change `findValue` to be the thumbprint of your client certificate.

After you reset IIS, ControlPoint requests and is accessible using the created certificates.

Redeploy ControlPoint when HTTPS is enabled

If you need to redeploy ControlPoint, then you must change HTTP to HTTPS in the configuration files.

You must change HTTP back to HTTPS in the **https** service section of the Dashboard, Timer, and WebService `web.config` file.

Configure the Redirector service for HTTPS

The ControlPoint Redirector service is used to redirect users to a shortcut of a document created using a Secure Shortcut policy.

NOTE: Shortcut redirection to the new location supports only IE browsers.

To access a redirect link securely, you must configure the service for HTTPS.

To configure the Redirector service for HTTPS

1. [Create certificates.](#)
2. [Bind certificate with a port.](#)
3. [Configure the Redirector service for HTTPS.](#)

Create certificates

You must create a certificate authority (CA) to sign the server certificates. These certificates are required for authentication.

NOTE: When generating the certificates, do not use the SHA-1 algorithm as it has been deprecated.

To create certificates

1. Import the cer file for the Certificate Authority to the Local Computer's Trusted Root Certification Authorities.
2. Import the cer file for the Server certificate to the Local Computer's Personal certificate store.

Bind certificate with a port

After creating the certificate, bind it to Redirector service port 7050.

To bind the certificate

1. Open PowerShell and run the following command:

```
netsh http add sslcert iport=<LocalhostIP>:7050 certhash=<Thumbprint of a server certificate> appid=<GUID of application>
```

Example

```
netsh http add sslcert iport=10.10.10.1:7050  
certhash=6b58bff0b663d452a32bdcdf4ba72ba8f18ce79 appid={4f3f8d5c-c5a9-4ecc-85fb-b17db658f246}
```

NOTE: The appid for Redirector service is: {4f3f8d5c-c5a9-4ecc-85fb-b17db658f246}

Configure the Redirector service for HTTPS

To edit the Redirector service configuration file

1. Open the \Program Files\Micro Focus\ControlPoint\Engine\Scheduler\ControlPointTimer.exe.config file in a text editor.

2. Add the following parameter:

```
<add key="RedirectorHttps" value="false"/>
```

For HTTPS, set the parameter to "true".

3. Save the file.

4. Open the Program Files\Micro Focus\ControlPoint\Engine\Redirector.exe.config file in a text editor.

5. Add the following parameters:

```
<add key="SecurePorts" value="false"/>  
<add key="RedirectorHttps" value="false"/>
```

For HTTPS, set the parameters to "true".

6. Save the file.
7. Restart the Redirector service and ControlPoint Engine service.

Chapter 7: Install the ControlPoint Edge File System connector

The Edge File System connector is used to run Archive policies on documents and files located on Windows file shares. This chapter describes how to install the Edge File System connector. It also provides information about how to uninstall it.

To install the ControlPoint Edge File System connector

1. [Install ControlPoint Edge File System Connector software](#)
2. [Configure the Edge File System Connector for HTTPS](#)

Install ControlPoint Edge File System Connector software

To run archive policies, you need to install the ControlPoint Edge File System Connector.

Before you begin

Ensure the following:

- The ControlPoint software is installed and configured.
- The server for the Edge File System Connector meets all hardware, software, and third-party component requirements listed in the *ControlPoint Support Matrix*. You can find this document on the [Micro Focus ControlPoint documentation site](#).

To install the ControlPoint Edge File System Connector

1. Run the ControlPoint Edge File System Connector installer, ControlPoint File System Agent Installer.exe.

You can find the installer at ControlPoint<version>\Agents\ControlPoint File System Agent\Windows.

The setup wizard appears.

2. Click **Next**.

The Log Directory page opens.

3. Select a directory for the installation setup log files, and click **Next**.

The Installation Location page opens.

4. Specify a location to install the Edge File System Connector software.
The default installation location is C:\Program Files\Micro Focus\ControlPoint\Edge.
5. Click **Next**.
The Server page opens.
6. Specify the name of the ControlPoint server.
The ControlPoint Edge File System Connector service needs to connect to this ControlPoint server to execute the archive policies.
7. For ControlPoint environments running with HTTPS, click **HTTPS Enabled**.
8. If you enabled the Advanced IDOL Distribution feature through the Configuration Manager and IDOL Deploy Tool, select the **Advanced IDOL Distribution** check box.
9. Click **Next**.
The Service User page opens.
10. Specify the credentials that will be used to run the ControlPoint Edge File System Connector services and to connect to the ControlPoint server.
11. Click **Next**.
The Installation Confirmation page opens.
12. Click **Install**.
After the connector is installed, you are prompted to restart the system to complete the installation.

Configure the Edge File System Connector for HTTPS

The ControlPoint Edge File System Connector configuration file for Windows contains the following "EnableSSL" config section, which is disabled by default.

```
[EnableSSL]  
SSLEnabled=false
```

If IDOL on the ControlPoint server is already using HTTPS, you should set `SSLEnabled` to `true` so the ControlPoint Edge File System Connector appears in the connection list on the Repository page of the ControlPoint Dashboard.

All other HTTPS configurations to run the ControlPoint Edge File System Connector on HTTPS are similar to the configuration of a regular File System connector.

Uninstall the Edge File System connector

To uninstall the ControlPoint Edge File System Connector

1. Uninstall the Edge File System Connector and then the archive service from the Windows **Add/Remove** Programs option.
2. Restart the system.

Chapter 8: Optimize IDOL configuration

NOTE: This content is applicable only to ControlPoint Content. The following section includes limited and specific information on IDOL server configuration parameters, which can help you optimize the configuration for ControlPoint.

For detailed information on these parameters, see the *IDOL Server Reference Guide*, available from the [Micro Focus IDOL documentation site](#).

To make the analysis process efficient and fast, you must optimize your IDOL configuration.

Modify the following parameters to optimize the configuration:

Parameter	Description
SplitNumbers	<p>Use this parameter to reduce the analysis size and RAM consumption, which will speed up analyzing.</p> <p>Set SplitNumbers to False if you need numeric wild card searching.</p> <p>Example:</p> <pre>SplitNumbers=false</pre>
FlushLockFile	<p>Use this parameter to specify the lock file, which prevents two or more analyzing engines that share the same physical disk from flushing at the same time. This will speed up analyzing substantially.</p> <p>Example:</p> <pre>FlushLockFile=\\host1\Lock\SanLockFileHost1.txt</pre> <p>Even when an IDOL server is using physical disks, where multiple Content Engines are using storage on the same physical drive channel, this setting prevents concurrent flushing.</p> <p>As an example, on a server with three independent RAID arrays, all the Content Engines on each disk should share a lock file. You can trigger this behavior by adding this parameter to each Content Engine's configuration.</p>
IndexCacheMaxSize	<p>Use this parameter to determine how much memory the IDOL Server uses to cache data for analyzing. It is available under the [IndexCache] section of the IDOL Server configuration file.</p> <p>Example:</p>

Parameter	Description
	<p data-bbox="634 289 797 317">[IndexCache]</p> <p data-bbox="634 338 967 365">IndexCacheMaxSize=102400</p> <p data-bbox="634 386 1344 449">Setting the IndexCacheMaxSize option requires knowledge of the system.</p> <ul data-bbox="634 470 1377 617" style="list-style-type: none"><li data-bbox="634 470 1333 497">• If IndexCacheMaxSize is too small, indexing becomes slow.<li data-bbox="634 518 1377 617">• Ideally IndexCacheMaxSize = amount of free RAM. However, if IndexCacheMaxSize is greater than the amount of free RAM, it pages the RAM to disk, which slows the system.

Chapter 9: Configure IDOL for HTTPS

This section provides information about the following tasks related to configuring IDOL for HTTPS:

- [Configure IDOL and connectors for HTTPS](#)
- [Stop IDOL services running with HTTPS](#)
- [Run ControlPoint Configuration Manager with HTTPS enabled](#)
- [Troubleshooting](#)

Configure IDOL and connectors for HTTPS

To establish secure connection with IDOL and connectors, complete the following tasks.

1. [Create SSL certificates](#) in the environment.
2. [Update the IDOL configuration](#).
3. [Configure ControlPoint to enable IDOL in HTTPS mode, on page 71](#).

Create SSL certificates

To create the SSL certificates

1. Create a self-signed Certificate Authority (CA) certificate.
2. Create a server key and server certificate signed by CA.
3. Copy these certificates to a directory that can be accessed by the ControlPoint installation.

Update the IDOL configuration

NOTE: The IDOL configuration files may not contain some of the sections by default. These sections must be added manually to the configuration files.

To update the IDOL configuration

1. Stop the IDOL, Connector, and ControlPoint related services using one of the following methods:
 - **HTTP environment.** As the local administrator, run `_stop_service.bat`, which is located in `\temp\ControlPoint\host_<hostName>`

- **HTTP or HTTPS environment.** Using Services, manually stop the services in the following order:
 - `<connectorName>` Service
 - `<connectorName>` Connector Framework Service
 - Distributed Connector Service
 - MetaStore Service
 - IDOL Service
 - OGS Service
 - Statistics Service
 - Content Service
 - LicenseServer Service
- 2. Modify the configuration (`.cfg`) files located in the installation directory as shown in the subsequent sections of this step.

For example, Program Files\Micro Focus\ControlPoint\Indexer.

The default or generic configuration files are:

- `agentstore.cfg`
- `ControlPoint Content.cfg`
- `ControlPoint DataAnalysis Store.cfg`
- `ControlPoint Distributed Connector.cfg`
- `ControlPoint <connectorName> Connector.cfg`
- `ControlPoint <connectorName> Connector Framework.cfg`
- `ControlPoint IDOL.cfg`
- `ControlPoint OGS.cfg`

NOTE: Depending on the number of connectors in the environment, there may be additional configuration files. Update the corresponding connector configuration files in the same manner as the `ControlPoint File System Connector.cfg` file.

agentstore.cfg

- a. Open Program Files\Micro Focus\ControlPoint\Indexer\IDOL\agentstore\agentstore.cfg in a text editor.
- b. Create a new section that adds the location of the server certificate and server key:

```
[SSLOption0]
SSLMethod=TLSV1.2
```

```
SSLCertificate=<location>\server.crt  
SSLPrivateKey=<location>\server.key
```

- c. In each of the following sections, add the lines shown:

[Server] section

```
SSLConfig=SSLOption0  
SSLIDOLComponents=TRUE
```

[Service] section

```
SSLConfig=SSLOption0
```

[IndexServer] section

```
SSLConfig=SSLOption0
```

- d. Save the file.

ControlPoint Content.cfg

- a. Open Program Files\Micro Focus\ControlPoint\Indexer\Content\ControlPoint Content.cfg in a text editor.
- b. Create a new section that adds the location of the server certificate and server key:

```
[SSLOption0]  
SSLMethod=TLSV1.2  
SSLCertificate=<location>\server.crt  
SSLPrivateKey=<location>\server.key
```

- c. In each of the following sections, add the lines shown:

[Server] section

```
SSLConfig=SSLOption0
```

[Service] section

```
SSLConfig=SSLOption0
```

[IndexServer] section

```
SSLConfig=SSLOption0
```

- d. Save the file.

ControlPoint DataAnalysis Store.cfg

- a. Open Program Files\Micro Focus\ControlPoint\Indexer\Statistics\ControlPoint DataAnalysis Store.cfg in a text editor.
- b. Create a new section that adds the location of the server certificate and server key:

```
[SSLOption0]  
SSLMethod=TLSV1.2
```

```
SSLCertificate=<location>\server.crt  
SSLPrivateKey=<location>\server.key
```

- c. In each of the following sections, add the lines shown:

[Server] section

```
SSLConfig=SSLOption0
```

[Service] section

```
SSLConfig=SSLOption0
```

[IndexServer] section

```
SSLConfig=SSLOption0
```

- d. Save the file.

ControlPoint Distributed Connector.cfg

- a. Open Program Files\Micro Focus\ControlPoint\Indexer\Distributed Connector\ControlPoint Distributed Connector.cfg in a text editor.
- b. Create a new section that adds the location of the server certificate and server key:

```
[SSLOption0]  
SSLMethod=TLSV1.2  
SSLCertificate=<location>\server.crt  
SSLPrivateKey=<location>\server.key
```

- c. In each of the following sections, add the lines shown:

[Server] section

```
SSLConfig=SSLOption0
```

[Service] section

```
SSLConfig=SSLOption0
```

[IndexServer] section

```
SSLConfig=SSLOption0
```

[Idol] section

```
SSLConfig=SSLOption0
```

[Fetch] section

```
SSLConfig=SSLOption0
```

[DistributedConnector] section

```
ConnectorSSLConfig=SSLOption0
```

```
SSLConfig=SSLOption0
```

ViewServer section

```
SSLConfig=SSLOption0
```

- d. Save the file.

ControlPoint xxx Connector.cfg

- a. Open Program Files\Microsoft Focus\ControlPoint\Indexer\xxx Connector\ControlPoint xxx Connector.cfg a in text file.

Where xxx is the connector name.

- b. Create a new section that adds the location of the server certificate and server key:

```
[SSLOption0]  
SSLMethod=TLSV1.2  
SSLCertificate=<location>\server.crt  
SSLPrivateKey=<location>\server.key
```

- c. In each of the following sections, add the lines shown:

[Server] section

```
SSLConfig=SSLOption0
```

[Service] section

```
SSLConfig=SSLOption0
```

[IndexServer] section

```
SSLConfig=SSLOption0
```

[Fetch] section

```
SSLConfig=SSLOption0
```

[ViewServer] section

```
SSLConfig=SSLOption0
```

[FetchTasks] section

```
SSLConfig=SSLOption0
```

[DistributedConnector] section

```
SSLConfig=SSLOption0
```

[Ingestion] section

```
IngestSSLConfig=SSLOption0
```

[Connector] section

```
IngestSSLConfig=SSLOption0
```

- d. Save the file.

NOTE: Similarly, other connector cfg files can be modified to enable a secure connection.

ControlPointxxx Framework.cfg

- a. Open Program Files\Microsoft Focus\ControlPoint\Indexer\xxx Connector Framework\ControlPoint xxx Framework.cfg in a text editor.

Where xxx is the connector name.
- b. Create a new section that adds the location of the server certificate and server key:

```
[SSLOption0]
SSLMethod=TLSV1.2
SSLCertificate=<location>\server.crt
SSLPrivateKey=<location>\server.key
```
- c. In each of the following sections, add the lines shown:

```
[Server] section
SSLConfig=SSLOption0
```

```
[Service] section
SSLConfig=SSLOption0
```

```
[MyIdolIndexer] section
SSLConfig=SSLOption0
```

```
[Categorizer] section
SSLConfig=SSLOption0
```

```
[MyMetaStoreIndexer] section
SSLConfig=SSLOption0
```
- d. Save the file.

NOTE: Similarly, other connector cfg files can be modified to enable a secure connection.

- e. Edit the category.lua file for the Connector Framework

To edit the LUA file on each Connector Framework

- i. Navigate to the file location:

```
Program Files\Microsoft Focus\ControlPoint\Indexer\<connectorFramework>\lua\Category.lua
```

For example:

```
Program Files\Micro Focus\ControlPoint\Indexer\FileSystem Connector  
Framework\lua\Category.lua
```

- ii. Search for the line:

```
local categorize = document:getFieldValue("AUTN_CATEGORIZE",false)
```

- iii. Insert a new statement after the statement in step 2:

```
local sslParameters =  
{  
    SSLMethod = "TLSV1.2",  
}
```

- iv. Edit the line:

```
local xmlString = send_aci_action(hostName, port,  
"CategorySuggestFromText", {querytext = content, NumResults =  
maxCategories, textparse = "true", agentBoolean = "true", anylanguage =  
"true", FieldText = "NOT EXISTS{:CONTAINERCAT AND NOT EXISTS  
{:SHADOWCATEGORYOF}"}, timeout, retries )
```

to

```
local xmlString = send_aci_action(hostName, port,  
"CategorySuggestFromText", {querytext = content, NumResults =  
maxCategories, textparse = "true", agentBoolean = "true", anylanguage =  
"true", FieldText = "NOT EXISTS{:CONTAINERCAT AND NOT EXISTS  
{:SHADOWCATEGORYOF}"}, timeout, retries, sslParameters )
```

- v. Save the file.

ControlPoint IDOL.cfg

- a. Open Program Files\Micro Focus\ControlPoint\Indexer\IDOL\ControlPoint IDOL.cfg in a text editor.
- b. Create a new section that adds the location of the server certificate and server key:

```
[SSLOption0]  
SSLMethod=TLSV1.2  
SSLCertificate=<location>\server.crt  
SSLPrivateKey=<location>\server.key
```

- c. In each of the following sections, add the lines shown:

[Server] section

```
SSLIDOLComponents=TRUE  
SSLConfig=SSLOption0
```

[Service] section

```
SSLConfig=SSLOption0
```

[DataDRE] section

SSLConfig=SSLOption0

[CatDRE] section

SSLConfig=SSLOption0

[AgentDRE] section

SSLConfig=SSLOption0

[Viewing] section

SSLConfig=SSLOption0

[IndexServer] section

SSLConfig=SSLOption0

[Agent] section

SSLConfig=SSLOption0

IndexSSLConfig=SSLOption0

NOTE: If you are working on a unified DIH/DAH environment, then all the DIH/DAH related configurations will be present in the `IDOL.cfg` file.

[DAHEngine0] section

SSLConfig=SSLOption0

[DIHEngine0] section

SSLConfig=SSLOption0

ServiceSSLConfig=SSLOption0

NOTE: This setting enables DIH to communicate securely with child engines.

[Autonomy] section

SSLConfig=SSLOptions0

[Notes] section

SSLConfig=SSLOptions0

[LDAP] section

SSLConfig=SSLOptions0

[Documentum] section

SSLConfig=SSLOptions0

[Exchange] section

SSLConfig=SSLOptions0

[Trim] section

SSLConfig=SSLOptions0

[SharePoint] section

SSLConfig=SSLOptions0

[NT] section

SSLConfig=SSLOptions0

- d. Save the file.

ControlPoint MetaStore.cfg

- a. Open Program Files\Micro Focus\ControlPoint\Indexer\metaStore\ControlPoint Metastore.cfg in a text editor.
- b. Create a new section that adds the location of the server certificate and server key:

[SSLOption0]

SSLMethod=TLSV1.2

SSLCertificate=<location>\server.crt

SSLPrivateKey=<location>\server.key

- c. In each of the following sections, add the lines shown:

[Server] section

SSLConfig=SSLOption0

[Service] section

SSLConfig=SSLOption0

[IndexServer] section

SSLConfig=SSLOption0

[Actions] section

SSLConfig=SSLOption0

[IngestAction] section

SSLConfig=SSLOption0

- d. Save the file.

ControlPoint OGS.cfg

- a. Open Program Files\Micro Focus\ControlPoint\Indexer\OGS\ControlPoint OGS.cfg in a text editor.
- b. Create a new section that adds the location of the server certificate and server key:

[SSLOption0]

SSLMethod=TLSV1.2

```
SSLCertificate=<location>\server.crt  
SSLPrivateKey=<location>\server.key
```

- c. In each of the following sections, add the lines shown:

[Server] section

```
SSLConfig=SSLOption0
```

[Service] section

```
SSLConfig=SSLOption0
```

Default section

```
GroupServerSSLConfig=SSLOption0
```

- d. Save the file.

3. Start the IDOL, Connector and ControlPoint related services using one of the following methods:
- **HTTP environment.** As the local administrator, run `_start_service.bat`, which is located in `\temp\ControlPoint\host_<hostName>`
 - **HTTP or HTTPS environment.** Manually start the services in the following order:
 - LicenseServer Service
 - Content Service
 - Statistics Service
 - OGS Service
 - IDOL Service
 - Distributed Connector Service
 - `<connectorName>` Connector Framework Service
 - `<connectorName>` Connector Service
 - MetaStore Service
4. If there are any additional connectors or connector framework configuration files configured with SSL, then start them manually.
5. Restart the related services to access all ports securely.

Configure ControlPoint to enable IDOL in HTTPS mode

To configure ControlPoint to enable IDOL in HTTPS mode

1. Stop the application pool for the ControlPoint website in IIS.
2. Stop ControlPoint Engine in Services.

3. In the appSettings section of the following files:

- Program Files\Micro Focus\ControlPoint\Dashboard\Web.config
- Program Files\Micro Focus\ControlPoint\DataAnalysis\Agent\Autonomy.ControlPoint.DataAnalysis.Controller.BundledAgent.exe.config
- Program Files\Micro Focus\ControlPoint\DataAnalysis\Service\Web.config
- Program Files\Micro Focus\ControlPoint\DataAnalysis\SqlAgent\Autonomy.ControlPoint.DataAnalysis.Controller.BundledSqlAgent.exe.config
- Program Files\Micro Focus\ControlPoint\Engine\CallBack\Web.config
- Program Files\Micro Focus\ControlPoint\Engine\Scheduler\ControlPointTimer.exe.config
- Program Files\Micro Focus\ControlPoint\MvcWeb.config
- Program Files\Micro Focus\ControlPoint\WebService\Web.config

Make the following changes:

a. Remove the following line (if it exists):

```
<add key="MetaStorePort" value="4500" />
```

b. Add the following to configure IDOL setup to use HTTPS mode:

```
<add key="SecurePorts" value="true"/>
```

4. In the appSettings section of the following files:

- Program Files\Micro Focus\ControlPoint\Dashboard\web.config
- Program Files\Micro Focus\ControlPoint\WebApi\web.config

Remove the following line (if it exists):

```
<add key="OgsHttpQuery" value="localhost:4057" />
```

5. Start the ControlPoint website in IIS.
6. Start ControlPoint Engine in Services.
7. If required, restart the server for a clean start of all services.

NOTE: If you uninstall and reinstall ControlPoint software for any reason, the changes to configure IDOL for HTTPS are lost. You will need to repeat the preceding steps.

Stop IDOL services running with HTTPS

To stop individual services when IDOL is running with HTTPS:

1. Open Services on Windows and select the service that needs to be stopped.
2. Right-click the service and click **Stop**.
3. Stop the following services in order:
 - FileSystem Connector
 - MetaStore
 - Distributed Connector
 - FileSystem Connector Framework
 - IDOL

NOTE: This stops the IDOL proxy server. To stop the sub processes of IDOL, see the next step.

- OGS
 - Statistics
 - Content
 - LicenseServer
4. In Task Manager, stop the following IDOL child processes:
 - agentstore.exe
 - category.exe
 - community.exe
 - dah.exe
 - dih.exe
 - view.exe

Run ControlPoint Configuration Manager with HTTPS enabled

NOTE: You can configure IDOL to use HTTPS and can configure ControlPoint to use either HTTP or HTTPS.

If you configured all IDOL components and connectors to work with HTTPS, then you must perform the following steps:

1. Import the Certificate Authority (CA) certificate (created for the IDOL SSL setup) to the Microsoft Management Console under **Trusted Root Certification Authorities** on your local computer.
2. Open the Microsoft Management Console. You can also run `mmc.exe` from **Start > Run**.
3. From the File menu, click **Add/Remove Snap-in**.

The Add / Remove Snap-in window appears.

4. Select **Certificates** from the Available snap-ins pane and click **Add**, and then click **OK**.
5. In the Certificates snap-in window, select **Computer account**, and then click **Next** to finish.
6. In the Microsoft Management Console, right-click the **Trusted Root Certificate Authority**, select **All Tasks** and **Import**.

The Certificate Import Wizard window appears.

7. Browse to select the CA certificate and click **Finish**.

A confirmation window appears after successfully importing the certificate.

8. In the Program Files\Microsoft Focus\ControlPoint\Configuration\ControlPointConfiguration.exe.config file, configure the following line in the appSettings section.

```
<add key="SecurePorts" value="true" />
```

9. Launch the ControlPoint Configuration Manager, and then click **Deploy**.

Troubleshooting

This chapter provides troubleshooting information related to IDOL integration with ControlPoint.

Verify HTTPS setup for IDOL

Description

Verify that all the ports are up and running with HTTPS.

Solution

1. Modify the configuration files for connectors and IDOL with SSL settings.
2. Verify that all the ports are up and running with HTTPS. Run the following commands:
 - a. DC port : `https://localhost:7000/a=getstatus`
 - b. File system connector : `https://localhost:7200/a=getstatus`
 - c. IDOL port: `https://localhost:9000/a=getstatus`
 - i. Category DRE: `https://localhost:9020/a=getstatus`
 - ii. Community: `https://localhost:9030/a=getstatus`
 - iii. agentstore: `https://localhost:9050/a=getstatus`
 - iv. DAH: `https://localhost:9060/a=getstatus`
 - v. DIH : `https://localhost:9070/a=getstatus`

```
<engine>
  <number>0</number>
  <group>0</group>
  <host>TestVM</host>
  <port>32000</port>
  <status>UP</status>
  <updateonly>>false</updateonly>
  <weight>1</weight>
  <disabled>>false</disabled>
</engine>
```
 - vi. Verify the status of the engine. It should be up and running.
View: `https://localhost:9080/a=getstatus`
 3. Content Engine : `https://localhost:32000/a=getstatus`
 4. DataAnalysis DataStore: `https://localhost:31500/a=getstatus`
 5. Similarly, for other connectors that are installed, perform a check on the respective port numbers.

Port numbers can be found in the configuration file under the [Server] section.

Repository page does not list registered repositories after changing the IDOL setup on HTTPS

Problem

You have registered repositories, but after changing the IDOL setup on HTTPS, the repository page is not listing the registered repositories.

Description

This issue could happen in the following circumstances:

1. A caching issue in the browser.
2. A repository created with a connector, which is not configured with SSL settings. The repository page makes a call to `ListConnectors` and waits for all connectors with repositories to return.

Solutions

- Clear the browser cache and reload the page.
- Verify the SSL settings in the connector configuration file.

ControlPoint Configuration Manager cannot establish trust relationship

Problem

The ControlPoint Configuration Manager displays the following error message when you click **Deploy**.

```
Could not establish trust relationship for the SSL / TLS secure channel
```

Solution

1. Ensure that the CA certificate for IDOL is imported to the Trusted root authority certificate store on your local computer.
2. Double click the certificate file to verify the details of the Server certificate for IDOL.
3. Ensure that ControlPoint Configuration Manager has the same name as provided in the certificate on the host for DataAnalysis, IDOL server settings and for MetaStore.

Chapter 10: Set up IDOL distributed mirror / non-mirror modes

This chapter describes the procedure to set up multi-layer IDOL DIH/DAH to get better performance and scalability.

- [Introduction](#)
- [Set up mirror mode](#)
- [Set up non-mirror simple combinator mode](#)
- [Add exception in Windows Firewall](#)

Introduction

The Distributed Handler mode is generally installed when an organization wants to employ a fail-over, load-balanced or combined fail-over or load-balanced architecture. It is common practice to install the Distributed Handler mode when organizations own large quantities of data, which need to be indexed into the IDOL server.

This requires the installation of multiple distributed content engines to support the large quantities of documents that need to be indexed into the meaning-based computing layer of IDOL.

For more information, see the Distributed Handlers training material, and the Distributed Setup section in the *IDOL Getting Started*, *Micro Focus DIH Administration*, and *Micro Focus DAH Administration* guides.

Set up mirror mode

To set up mirror mode with one tier DIH/DAH and two content engines

1. Install IDOL and ControlPoint.
Select two content engines when running ControlPoint IDOL Deploy Tool.exe.
2. Stop the ControlPoint IDOL service.
3. Navigate to the IDOL installation path at the following location:
C:\Program Files\Micro Focus\ControlPoint\Indexer\IDOL.

4. Open ControlPoint IDOL.cfg and remove or comment VirtualDatabases and all [vdb], as shown in the following example:

```
//VirtualDatabases=2  
//[vdb0]  
//DbName=News  
//Internal=False  
//Type=combinator  
//MapsTo=0:News,1:News  
//[vdb1]  
//DbName=Archive  
//Internal=False  
//Type=combinator  
//MapsTo=0:Archive,1:Archive
```

5. Change the following parameters:

Section	Parameter	Value
[DistributionSettings]	DistributeByReference	FALSE
	UseConsistentHashing	false
	MirrorMode	true

6. Navigate to the IDOL DIH installation path:
C:\Program Files\Micro Focus\ControlPoint\Indexer\IDOL\dih
7. Delete the main directory.
8. Start the ControlPoint IDOL service.

Set up non-mirror simple combinator mode

The structure for the non-mirror simple combinator mode is similar to the mirror mode setup. This section explains the tasks needed for non-mirror simple combinator mode, with examples.

1. Configure three virtual machines as required using Windows Server.
2. On the first virtual machine (VM1), install ControlPoint and IDOL with one content engine.
If you have ControlPoint and IDOL on different systems, then the IDOL deployment host should be on VM1.
3. Install IDOL DIH/DAH and the three content engines on the other two virtual machines (VM2 and VM3).
4. On all three virtual machines, modify the host file (C:\Windows\System32\drivers\etc) to include all of the IP addresses and host names in the host file.

5. Install ControlPoint and IDOL.

CAUTION: Do not delete the IDOL deploy temp directory. You need to copy the content engine software from here.

6. Open the browser query control URL and ensure that it works without any problems.
7. Stop the IDOL services by navigating to the dih and dah directories available at the following location:

`%IDOL_INSTALL_PATH%\Indexer\IDOL`

Run the following command:

`run _cleanup.dat`

8. Remove all of the Content Engine services that are managed by the first tier DIH / DAH.
From the content engine directory, as the local administrator, run the `_stop_service.bat` and `_uninstall_service.bat` batch files.

9. Copy the Standlone DIH DAH directory available at the following location:

`ControlPoint\Standlone DIH DAH)`

As the local administrator, run the batch files:

- `DIH_install_service.bat`. DIH is installed as a Windows service.
- `DAH_install_service.bat`. DAH is installed as a Windows service.

10. For the content engine, copy the following directories from the IDOL temp directory to VM2 and VM3:

- Content directory: `temp\ControlPoint\host_hostName\Indexer .`
- langfiles directory: `temp\ControlPoint\host_hostName\Commons\langfiles.`

11. Run the script to install the engine service.
12. If more than one content engine is required, then do the following:
 - a. Rename the content engine executable (`.exe`) file and the configuration (`.cfg`) file.
 - b. Update the `LanguageDirectory` in the configuration file.
 - c. Update the batch scripts in the content directory.
13. Edit the DAH configuration files on VM2 and VM3 to enable non-mirror simple combinator mode. In this mode, DAH does not need to set up the virtual database.

Modify as shown:

Section	Parameter	Value
---------	-----------	-------

[Service]	ServiceStatusClients	*.*.*.*
	ServiceControlClients	*.*.*.*
	Access-Control-Allow-Origin	*
[Server]	AdminClients	*.*.*.*
	QueryClients	*.*.*.*
	IndexClients	*.*.*.*
	MirrorMode	False
	SimpleCombinatorMode	true

14. In the [DistributionIDOLServers]section, configure the content engines.

```
[Service]
ServicePort=9062
ServiceStatusClients=*.*.*.*
ServiceControlClients=*.*.*.*
Access-Control-Allow-Origin=*
XSLTemplates=TRUE
[Server]
Port=9060
AdminClients=*.*.*.*
QueryClients=*.*.*.*
IndexClients=*.*.*.*
MirrorMode=FALSE
SimpleCombinatorMode=true
[DistributionIDOLServers]
Number=3
[IDOLServer0]
Host=localhost
Port=32000
[IDOLServer1]
Host=localhost
Port=32050
[IDOLServer2]
Host=localhost
Port=33000
```

15. Edit the DIH configuration files on VM2 and VM3.

Modify as shown:

Section	Parameter	Value
---------	-----------	-------

[Service]	ServiceStatusClients	*.*.*.*
	ServiceControlClients	*.*.*.*
	Access-Control-Allow-Origin	*
[Server]	AdminClients	*.*.*.*
	IndexClients	*.*.*.*
	QueryClients	*.*.*.*
	MirrorMode	False

16. In the **[DistributionIDOLServers]** section, configure the content engines.

```
[Service]
ServicePort=9072
ServiceStatusClients=*.*.*.*
ServiceControlClients=*.*.*.*
Access-Control-Allow-Origin=*
[Server]
Port=9070
DIHPort=9071
AdminClients=*.*.*.*
IndexClients=*.*.*.*
QueryClients=*.*.*.*
MirrorMode=FALSE
DistributeByReference=TRUE
UseConsistentHashing=TRUE
[DistributionIDOLServers]
Number=3
[IDOLServer0]
Host=localhost
Port=32000
[IDOLServer1]
Host=localhost
Port=32050
[IDOLServer2]
Host=localhost
Port=33000
```

17. Modify the configuration file in the IDOL server on VM1.

Modify as shown:

Section	Parameter	Value
[DistributionSettings]	MirrorMode	false
	DistributionMethod	1

18. In the **[DAHEngines]** section, configure the DAH servers.

In the **[DIHEngine1]** section, configure the DIH servers.

```
[DistributionSettings]
DistributeByReference=TRUE
DistributeReplaceData=FALSE
UseConsistentHashing=FALSE
MirrorMode=false
DistributionMethod=1
[DAHEngines]
Number=2
[DAHEngine0]
Host=idol-child2
Port=9060
[DAHEngine1]
Host=idol-child3
Port=9060
[DIHEngines]
Number=2
[DIHEngine0]
Host=idol-child2
Port=9070
[DIHEngine1]
Host=idol-child3
Port=9070
```

19. Restart the IDOL server and then restart all DIHs, DAHs and content engine services in VM2 and VM3.
20. On VM2 and VM3, for each content engine, open `http://localhost:Content_Service_Port/a=getstatus` to verify if the status is SUCCESS.

NOTE: The port can be found in the content engine configuration file under `[server] Port=XXX`.

21. On VM2 and VM3, for each DIH / DAH, open `http://localhost: DIH/DAH_service_Port/a=getstatus` to verify if the status is SUCCESS.

All content engines that are managed by DIH/DAH will be listed and status should be Up.

NOTE: The port can be found in DIH/DAH configuration file under `[server] Port=XXX`.

22. On VM1, open `http://localhost:9000/a=getstatus` to verify Micro Focus IDOL server. Verify all components status are RUNNING.

Add exception in Windows Firewall

To enable DIH, DAH and the Content Engine in Windows firewall

1. Go to Firewall settings and Allow an app or feature through Firewall.
2. Click **Allow another application** and point to dih.exe, dah.exe and content engine.exe.
3. Click **Network types** and select all "Domain, public, private", then click **Add**. Repeat these steps in all the child nodes.

Chapter 11: Adjust antivirus software monitoring

For performance reasons, if you are running antivirus software on the ControlPoint host machines, ensure that it does not monitor the ControlPoint directories and any file shares that have been indexed.

Advanced antivirus software can scan the network and might block some ControlPoint traffic, which can cause errors.

Where possible, exempt the ControlPoint and IDOL processes from this kind of network traffic analysis.

Chapter 12: Update DataAnalysis configurations after IIS hardening

If you enabled the Extended Protection for Authentication mechanism in IIS for your DataAnalysis service, you must update the service's configuration file to ensure that you can access repositories through ControlPoint.

To update the DataAnalysis service configuration file

1. Open the `\Program Files\Micro Focus\ControlPoint\DataAnalysis\Service\web.config` file.
2. Locate the three instances of the following line:

```
<transport clientCredentialType="Windows" />
```

And replace each one with the following section:

```
<transport clientCredentialType="Windows" >  
  <extendedProtectionPolicy policyEnforcement="enforcementType" />  
</transport>
```

Where the value of *enforcementType* depends on the value you set for Extended Protection in IIS:

Extended Protection setting	<i>enforcementType</i> value
Accept	WhenSupported
Required	Always

3. Save the file.
4. Restart the DataAnalysis service using Windows Services.

Chapter 13: Upgrade ControlPoint

This chapter describes how to upgrade to ControlPoint 5.9.0 from a previous version.

NOTE: ControlPoint 5.9.0 supports upgrade from version 5.6 and later. To upgrade from an earlier version, first upgrade to version 5.6, and then upgrade to 5.9.0. Information about ControlPoint 5.6 is available from the [Micro Focus ControlPoint documentation site](#).

To upgrade ControlPoint

1. Ensure your environment meets all ControlPoint requirements, including the requirements for ControlPoint IDOL and connectors.

For information about the hardware, software, and third-party components necessary for ControlPoint and ControlPoint IDOL and connectors, see the *ControlPoint Support Matrix*. You can find this document on the [Micro Focus ControlPoint documentation site](#).

2. [Run the Support Utility](#).
3. [Note the current databases](#) for post-upgrade verification.
4. If your environment contains any SharePoint 2007, 2010, 2013, or HPE Content Manager connectors, [deactivate these deprecated connectors](#).

Starting with version 5.8.0, ControlPoint no longer supports these connectors.

5. [Prepare the ControlPoint environment for upgrade](#).
6. [Uninstall the current ControlPoint software](#).
7. [Upgrade to ControlPoint 5.9.0 software](#).
8. For environments with Edge File System connectors, [upgrade those connectors](#).
9. If your environment has NiFi IDOL Ingest libraries installed, [upgrade those libraries](#).
10. If you enabled ControlPoint security, update ControlPoint configuration files as described in [Configure ControlPoint security settings](#).
11. If the Extended Protection for Authentication mechanism in IIS is enabled for your DataAnalysis service, [update the DataAnalysis service's configuration file](#).

This step ensures that you can continue to access repositories through ControlPoint.

Run the Support utility

You can run the Support Utility before and after upgrade to compare the system information and configuration (.cfg and .config) file information to identify any differences.

For more information, see [ControlPoint Support utility, on page 156](#).

To run the Support utility

- Run the Support utility from the command line as the Administrator.

```
ControlPointSupportUtility.exe -c
```

The utility gathers a copy of all system and configuration file information and stores it labeled as Pre capture data in <systemroot>\Users*<user>*\AppData\Local\Temp.

Note the current databases

Before upgrading ControlPoint, make note of the current IDOL and MetaStore databases so that you can confirm they are available after upgrade.

To note the databases

1. Issue a GETSTATUS command for the following databases using HTTP or HTTPS, depending on which protocol your environment uses:
 - **IDOL:** `http|https://IDOLServerName:9000/a=getstatus`
 - **MetaStore:** `http|https://MetaStoreServerName:4500/a=getstatus`
2. Save the list of the databases displayed for future reference.

You will compare this list with the one you generate during the post-upgrade process.

Deactivate deprecated connectors

Starting with version 5.8.0, ControlPoint no longer supports the following connectors and their associated Connector Framework Service (CFS):

- HPE Content Manager Connector
- SharePoint 2007 Connector
- SharePoint 2010 Connector
- SharePoint 2013 Connector

If any of these connectors are active in your environment, you must manually deactivate the repositories related to each one.

NOTE: After upgrade, recapture data previously captured by the deprecated connectors by creating new repositories using the following ControlPoint IDOL connectors:

- Content Manager Trim Connector
- SharePoint Remote Connector

To deactivate a repository

1. Open the ControlPoint Console and go to the **Repositories** dashboard.
2. For the repository you want to remove:
 - a. Click , and then clear the **Execute Policy** check box.
 - b. If the repository was managed, also clear the **Assign Policy** check box.
 - c. Expand the **SCHEDULING** section, and under **CYCLE**, click **Run Once**.
 - d. Click **Save**.
3. Repeat step 2 for each additional repository you need to deactivate.

Prepare the ControlPoint environment for upgrade

Prepare the ControlPoint environment for the upgrade by disabling any scheduled tasks, stopping services, uninstalling software, and removing websites.

To prepare the environment

1. Allow any executing policy phases to complete.

NOTE: Ensure all items in the existing policies are in the executed or failed status, before the upgrade.

2. In the ControlPoint Administration dashboard, disable the **Assign Policies** and **Execute Policies** scheduled tasks using the **Scheduled Tasks** settings. This prevents new policies from being assigned to documents.

NOTE: Be sure to disable all of the scheduled tasks: Normal, Low, and High priority.

3. Ensure that all ingestion jobs are complete.

NOTE: If ingestion jobs are still running, wait for them to complete before proceeding.

4. Check the **Distributed Connector** queue by issuing one of the following commands, depending on whether the connector is working with HTTP or HTTPS:
 - `http://distributedConnectorHost:port/a=queueinfo&queuename=fetch&queueaction=getstatus`
 - `https://distributedConnectorHost:port/a=queueinfo&queuename=fetch&queueaction=getstatus`

The default port number is 7000.

All actions should be Finished.

5. When all connector actions and executing policy phases have completed, stop the following services:

- ControlPoint Engines
- Distributed Connector
- Individual connectors and Connector Framework Services

6. Back up the following folders so you can reapply existing values from them after upgrade:

- Program Files*<companyName>*\ControlPoint\Indexer

This folder contains subfolders with IDOL and connector configuration files (.cfg) and statistic files (.db).

- If your environment contains Insert Configurations:

Program Files*<companyName>*\ControlPoint\InsertConfig

Where *<companyName>* is one of the following, depending on your previous version of ControlPoint software:

Autonomy, Hewlett Packard, Hewlett Packard Enterprise, or Micro Focus.

TIP: Files marked by a modification date later than the date of deployment indicates that it was modified manually or through the use of ControlPoint software.

7. Back up the ControlPoint databases:

- ControlPoint
- ControlPointAudit
- ControlPointMetaStore
- ControlPointMetaStoreTags
- ControlPointTracking
- ReportServer *(Available only if your environment is configured for reports)*
- ReportServerTempDB *(Available only if your environment is configured for reports)*

8. Start the SQL Server Agent service.

By default, the service is set to start manually. Change the service to start automatically and start the service now. The upgrade process requires it to be running.

After you have prepared the environment for upgrade, continue the upgrade with [Uninstall the current ControlPoint software, on the next page](#).

Uninstall the current ControlPoint software

After the environment is prepared, you can uninstall the current ControlPoint software and remove ControlPoint websites.

1. Uninstall the ControlPoint software using the Windows **Add/Remove Programs** option.

NOTE: The Add/Remove Programs dialog displays an option to retain or remove the FIPS security mode. Click **Yes** to retain the FIPS security mode, or **No** to remove it.

- If you select **Yes**, the ControlPoint installation will be considered as a fresh installation and you have the option to select or clear the **Enable FIPS security mode** check box.
- If you select **No**, the previous setting for **Enable FIPS security mode** is retained and you are not able to change its value. For more information, see [Enable Federal Information Processing Standards \(FIPS\) security mode, on page 43](#).

2. Remove the ControlPoint websites.
 - a. Identify all applications in the ControlPointAppPool140 application pool running on your Internet Information Services (IIS) and remove them.
 - b. Remove the ControlPointAppPool140 application pool.

It may include some or all of the following:

- ControlPoint
- Classifier
- CPWS
- Callback Handler
- Category
- Data Analysis Service
- WebAPI

The environment is ready for upgrade.

Upgrade to ControlPoint 5.9.0 software

The installers for the ControlPoint database and software are located in the ControlPoint installation package.

Before you begin

Ensure that the SQL Server Agent service is set for automatic start and that the service is running.

To upgrade to ControlPoint 5.9.0 software

1. [Upgrade ControlPoint databases to 5.9.0.](#)
2. [Install the ControlPoint software](#), which includes optionally enabling HTTPS.
3. [Upgrade IDOL data and software.](#)
4. [Complete the IDOL software upgrade manually.](#)
5. [Update configuration files](#) with settings from the previous environment.
6. If while upgrading IDOL you changed its location, [update IDOL files.](#)

To provide IDOL access to files generated or customized by the previous installation, manually copy them from the backup you created to the new IDOL location.

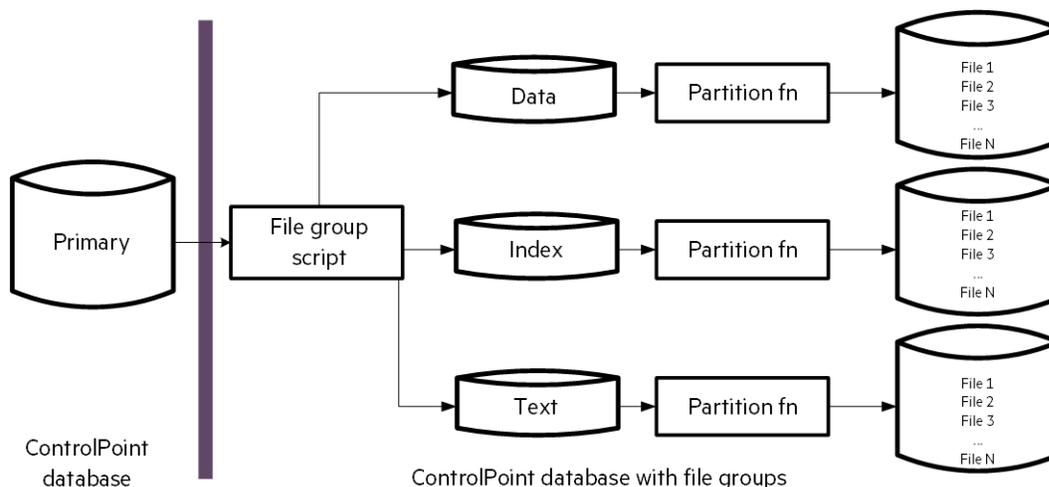
7. (Optional) [Reconfigure the Documentum connector.](#)

If you upgraded the Documentum connector, reconfigure it now.

8. [Perform post-upgrade steps.](#)
9. [Start Windows services.](#)
10. (Optional) [Configure Advanced IDOL Distribution.](#)

Upgrade ControlPoint databases to 5.9.0

ControlPoint 5.9.0 supports database partitions and file groups. If you are upgrading from a version that did not support those items, the following figure identifies how each ControlPoint database is upgraded and separated into file groups.



Prepare to upgrade ControlPoint databases

Before you upgrade the ControlPoint databases, there are a few tasks you must do to prepare your environment.

To prepare for database upgrade

1. [Verify the SQL Server sa account.](#)
2. [Configure minimum SQL permissions.](#)
3. [Grant permissions on database file locations.](#)
4. [Determine whether your database will require a DockKey update](#) after you upgrade your ControlPoint databases.

Verify the SQL Server sa account

Ensure that the SQL Server **sa** account exists with its regular class of permissions and is not disabled.

This account will own the ControlPoint database maintenance jobs the installation process creates. If the account is removed, renamed, or disabled, the steps that create maintenance jobs will fail.

Configure minimum SQL permissions

Ensure the user account that deploys or upgrades the ControlPoint databases has permissions equivalent to the **sysadmin** default SQL login role, including the following permissions configured in SQL Server:

- **Dbcreator, public.** Required to create the ControlPoint databases.
- **SecurityAdmin.** Required to create users in the ControlPoint databases.

NOTE: Db_owner permissions are the minimum SQL permissions that can be used after the initial deployment.

Grant permissions on database file locations

Grant the appropriate read and write permissions on the directories you will configure for the database file groups. Permissions include standard permissions on the objects and UAC access (usually controlled by ownership inheritance), if applicable.

Follow these guidelines:

- **When utilizing a SQL user account.** Read and write access (and UAC access) granted to both the user account that runs the database installation program on the SQL server and the user account that operates the SQL Server instance.
- **When utilizing a Windows user account.** Read and write access (and UAC access) granted to the user account that runs the installation program.

These are the minimum permissions and access controls required for the directory targets. You can allow additional access to the directories if necessary.

Determine whether a DocKey update is required

Complete this task to determine whether your ControlPoint database requires a DocKey update.

To determine whether a DocKey update is required

- In SSMS, while connected to the **ControlPointMetaStore** database using an **SA** (or equivalent account), execute the following SQL command:

```
select TargetTransformParams from [ControlPointMetaStore].[MetaStore].  
[MapColumn] WHERE SupportingTable = 'Metadata.ReferenceHash'
```

If the return value is:

- `<IgnoreCase>False</IgnoreCase>`, no DocKey update is required.
- `NULL`, you must update DocKey as instructed during the database post-upgrade task.

Upgrade the databases to 5.9.0

This task upgrades the ControlPoint databases to version 5.9.0.

TIP: The upgrade process also installs SQL Agent jobs that automatically perform database maintenance suitable for most environments. However, you can configure these jobs to better support very large databases. For more information, see the appendix for advanced database maintenance controls in the *ControlPoint Administration Guide*, which is available from the [Micro Focus ControlPoint documentation site](#).

Before you begin

Ensure that a data source in SQL Server Reporting Services is still configured from your previous installation. For more information, see [Configure the ControlPoint data source, on page 21](#).

To upgrade ControlPoint databases to 5.9.0

1. Navigate to the `\ControlPoint` directory and run `ControlPoint Database Installer.exe`.

NOTE: If Windows UAC is enabled on the server, ensure that the user account running the installation program is also a user account in SQL Server that has sufficient permissions to update databases and sufficient permission to the database file locations.

The database installer opens to the Welcome page.

2. Click **Next**.

The Log Directory page opens.

3. Change the path of the setup log file, if necessary, and then click **Next**.

The SQL Connection page opens.

4. Enter the required **SQL Server** and **instance** names, or select them from the list.

5. Select the required authentication method: **Windows** or **SQL Server**.

If you select **SQL Server Authentication**, enter a **Login ID** and **Password**.

6. If only one disk is present, clear the **Enable interleaving for database transactions** option.

This option, selected by default, automatically interleaves files from select file groups to multiple storage path targets. Paths that participate in the interleaving process are indicated on each of the following Database Configuration pages.

Files from within each of these file groups will be spread evenly across all the participating paths.

7. Click **Test Connection** to verify the server details.
8. In the **Job Owner Username** field, enter a SQL Server user name for an account that has System Administrator access to SQL Server.

NOTE: The ControlPoint Database installation program uses this account to create and configure several SQL Server Agent maintenance jobs.

This user account must exist in SQL Server; the installation program does not verify it exists.

9. Click **Next**.
10. On each of the next several Database Configuration pages, perform the following steps:
 - a. Specify the path to the files listed, and then click **Next**.

You will configure database files for the following:

- ControlPoint database
- ControlPointAudit database
- ControlPointMetaStore database
- ControlPointMetaStoreTags database
- ControlPointTracking database

NOTE: When specifying data paths, keep the following in mind:

- If you selected the option to interleave database transaction interleaving in step 6, each page indicates the paths participating in the interleaving.
- Specify paths local to the server where SQL Server is installed.
- Place Index files on a different volume than the other components in the file group.
- Place Log files on a different volume than the other database files.

- b. On the ControlPoint Export Database Configuration page, to create a database to hold ControlPoint data for BI analysis, select the option listed.

For information about populating this database if you select this option, see the BI analysis information in the *ControlPoint Administration Guide* (available from the [Micro Focus ControlPoint documentation site](#)) or ControlPoint Help Center.

11. Click **Next**.
 12. To confirm that you have backed up the databases before upgrade, on the Backup Confirmation page, click **I have backed up the databases**.
 13. Click **Next**.
- The ControlPoint Audit Reports page opens.
14. To upload audit reports to SQL Server Reporting Services (SSRS), select **Upload Reports** and click **Next**.

If you select **Upload Reports**, the Reports Configuration page opens.

- a. In the **Audit Reports Installation** area, enter the installation path in the **Install reports to** field.
- b. In the Report Manager Server Settings area, enter the following information:
 - i. **Report Manager URL**
 - ii. **Report Manager Virtual Directory**
 - iii. **Report Webservice Virtual Directory**

NOTE: For **Report Manager Virtual Directory** and **Report Webservice Virtual Directory**, enter the values you previously defined on the SSRS Configuration Manager's **Report Manager URL** and **Web Service URL** tabs, respectively.

15. Click **Next**.
16. Verify the details on the Installation Confirmation page, and click **Install**.

The databases are installed.

IMPORTANT: Several SQL scripts are run as part of the database installation. If the scripts encounter problems during execution, the database installation program displays a dialog box prompting you to **Retry** or **Abort**.

If you choose **Abort**, the installation program attempts to drop the databases. If it cannot drop the databases, you will need to perform the following steps:

- a. In SQL Server Management Studio, ensure that there are no temporary tables in the **dbo.Temp_DBNames** path.

System databases > msdb > Tables > dbo.Temp_DBNames
- b. Manually drop the affected ControlPoint databases.
- c. Manually drop the **tempdb** database.

Dropping the databases avoids inconsistencies resulting from incomplete script executions.
- d. Restore the ControlPoint databases from the backups you made during the preparation to upgrade.
- e. Restart the database installation program.

17. Review the installation log.
18. Either write down the hyperlinked connection string or click it to copy the string to your clipboard.

The ControlPointMetaStore service requires this connection string to access the **ControlPointMetaStore** database. You must save this connection string so you can use it during the [Configure deployment packages, on page 29](#) task to configure the ControlPointMetaStore component's SQL connection string to the MetaStore database.

19. Click **Finish**.

The installation wizard closes.

Database post-upgrade tasks

After the database upgrade completes, do the following:

1. If the **ControlPointMetaStore** and **tempdb** databases were not installed on dedicated hard drives, [move them to their own dedicated hard drives](#).

For example, ensure **ControlPointMetaStore** is located on its own dedicated drive and **tempdb** is located on its own dedicated drive.

2. If you previously determined that your database requires a DockKey update, [perform the DockKey update](#).
3. (Optional) [Configure the recovery model for ControlPoint databases](#).

The default recovery model for all ControlPoint databases is automatically set to SIMPLE. If necessary, you can change the recovery model to meet your needs.

Move ControlPoint databases

Due to high disk usage of the **ControlPointMetaStore** and **tempdb** databases, Micro Focus recommends that you allocate these databases their own dedicated hard drive.

For improved read and write performance of the **ControlPointMetaStore** database, Micro Focus also recommends the use of an enterprise-level solid-state drive (SSD).

NOTE: The following information illustrates how to move the **ControlPointMetaStore** and **tempdb** databases if they were not initially configured on dedicate hard drives.

The procedures are based on information provided in SQL Server documentation. For more information, see <https://docs.microsoft.com/en-us/sql/relational-databases/databases/move-user-databases?view=sql-server-2017>.

Example

This example describes how to move the **ControlPointMetaStore** and **tempdb** databases to dedicated hard drives E and F, respectively.

1. In SQL Server Management Console, run the following statement:

```
ALTER DATABASE ControlPointMetaStore SET OFFLINE;
```

IMPORTANT: The **tempdb** database cannot be set offline or online, so it is excluded from steps 1 and 4.

The database is set offline.

2. Move the file or files to the new location.

For example:

- Move ControlPointMetaStore.mdf to the E: volume
- Move tempdb.mdf to the F: volume.

3. For each file moved, run the following statement:

```
ALTER DATABASE ControlPointMetaStore MODIFY FILE ( name =  
ControlPointMetaStore_data, FILENAME =  
'E:\sqldata\ControlPointMetaStore.mdf' );
```

```
ALTER DATABASE tempdb MODIFY FILE ( name = tempdev, FILENAME =  
'F:\sqldata\tempdb.mdf' );
```

4. Run the following statement:

```
ALTER DATABASE ControlPointMetaStore SET ONLINE;
```

The database is set online.

5. Verify the file change by running the following query:

```
SELECT name, physical_name AS CurrentLocation, state_desc  
FROM sys.master_files  
WHERE database_id = DB_ID(N'ControlPointMetaStore');
```

```
SELECT name, physical_name AS CurrentLocation, state_desc  
FROM sys.master_files  
WHERE database_id = DB_ID(N'tempdb');
```

6. Stop and restart the instance of SQL Server for the change to take effect on **tempdb**.

Perform DocKey update

If you previously determined that your database requires a DocKey update, perform the update now.

The following table provides sizing information for three sample runs of the update. The update steps direct you to extrapolate from this chart the database and folder sizes you need to create based on the amount of data your ControlPoint environment contains.

Sample sizing data (best viewed at 100%)

Sample run	Hardware		Raw repository data	TempFolder .dat files	tempdb	ControlPointMetaStore database			
	CPU ¹	RAM				MetaStore. Document table rows	ControlPointMetadata. Eduction table rows	CPMetaStore DB + CPMetaStore DB log size	CPMetaStore DB log size (post-shrink)
Run 1									
Before patch	2 / 8	16 GB	68 GB	0 GB	8 MB	1187981	694755	12.68 GB	
After patch	2 / 8	16 GB	68 GB	3.17 GB	120.75 MB	1187981	694755	48.86 GB	15.17 GB
Run 2									
Before patch	2 / 8	64 GB	136 GB	0 GB	305.43 MB	2375481	26512082	26.31 GB	
After patch	2 / 8	64 GB	136 GB	8.50 GB	4407.5 MB	2375481	26512082	91.76 GB	28.07 GB
Run 3									
Before patch	2 / 8	64 GB	204 GB	0 GB	602.69 MB	3562981	52329409	39.94 GB	
After patch	2 / 8	64 GB	204 GB	15.33 GB	9643.04 MB	3562981	52329409	159.67 GB	43.26 GB

CPU¹: Virtual sockets / cores per socket

To perform the DocKey update

1. Open Microsoft SQL Server Management Studio (SSMS) and use the ControlPointdb_owner credentials to connect with SA (or equivalent account), then select the ControlPointMetaStore database.
2. Back up all ControlPoint databases.
3. Ensure that the drives where the following databases are installed have enough space to hold the following items generated during this update:

- tempdb database
- ControlPointMetaStore database plus the database's log files

NOTE: To estimate the space these items require, refer to the tempdb and CPMetaStore DB + CPMetaStore DB log size columns in the Sample sizing data (best viewed at 100%) table to extrapolate the values you need based on the sizes provided.

4. Use Microsoft SQL Server Management Studio (SSMS) to set the ControlPointMetaStore database's recovery mode to SIMPLE.

Make note of the recovery mode's original value so you can reset it later in this task.

5. Execute the ControlPoint\<version>\Utilities\DocKey Update Scripts\DocKeyUpdate.sql script.

This script requires two parameters:

- **Temporary folder.** A temporary folder with enough space to hold temporary data (.dat files) generated during this update. Create a temporary folder for this purpose, such as E:\Temp.

NOTE: To estimate the space the folder requires, refer to the **TempFolder .dat files** column in the [Sample sizing data \(best viewed at 100%\)](#) table to extrapolate the value you need based on the sizes provided.

Also, ensure the database user running the script has write privileges to the location you specify.

- **ControlPointMetaStore SQL server hostname.** The name of the SQL server that hosts the **ControlPointMetaStore** database.

NOTE: If you encounter an error while running any of these SQL scripts, do not continue. Instead, contact Support for help.

6. Back up the **ControlPointMetaStore** database.
7. Use SSMS to set the **ControlPointMetaStore** database's recovery mode to its original setting.
8. Execute the following SQL command in SSMS to shrink the **ControlPointMetaStore** database log files:

```
DBCC SHRINKFILE (ControlPointMetaStore_log, 1)
```

You will complete the DockKey update process by updating several configuration files later in the ControlPoint upgrade process.

Configure the recovery model for ControlPoint databases

The recovery model defines the type of transaction log the database maintains and therefore determines the restore options available should you need to restore the database. The default recovery model for all ControlPoint databases is automatically set to **Simple**. You can change the model to either **Full** or **Bulk-Logged** for each database to better meet your recovery needs.

To configure the recovery model

- For each ControlPoint, configure the recovery model using either SQL Server Management Studio or Transact-SQL.

For information about each type of recovery model and how to set one, see your SQL Server documentation.

Consider ControlPoint database partitioning and file groups

You should determine whether you want to take full advantage of the database partitioning and file groups that ControlPoint supports.

These features are especially important for the performance and scalability of large-scale ControlPoint environments.

For information on taking full advantage of SQL file groups and database partitioning with your ControlPoint databases, see the *ControlPoint Database Conversion Guide*. This guide details the advantages of converting the databases to using file SQL Server database partitioning and file groups, detailed conversion steps using database conversion scripts, and so on.

Install the ControlPoint software

After upgrading the ControlPoint databases, install the software.

To install the ControlPoint software

1. From the \ControlPoint directory, run Setup.exe as the Administrator, and then follow the instructions in the installer.
2. While the IDOL software from the previous version is still running, run the **Configuration Manager** to deploy ControlPoint:

- a. If IDOL is enabled with HTTPS in your environment, do the following:
 - i. Open the ControlPointConfiguration.exe.config file in a text editor.
 - ii. In the <appSettings> section, set the SecurePorts value to true:

```
<appSettings>
  <add key="SecurePorts" value="true"/>
</appSettings>
```
 - iii. Save the file.
- b. Run **Configuration Manager**.

For detailed steps about running Configuration Manager, see [Configure ControlPoint, on page 45](#).

The ControlPoint software installs.

NOTE: If ControlPoint was running on HTTPS before the upgrade and you want to enable it again, follow the instructions in [Enable HTTPS](#).

Upgrade IDOL data and software

Use this task to upgrade the IDOL data and software.

To upgrade the IDOL data and software

1. Run the **ControlPoint IDOL Upgrade** program and follow the instructions. The program is available from the following location:

Program Files\Micro Focus\ControlPoint\Engine\Scheduler\ControlPoint IDOL Upgrade.exe

Depending on which version of ControlPoint you are upgrading from, the ControlPoint IDOL Upgrade program might include one or more of the following steps:

- a. Back up IDOL.

NOTE: If you have an existing backup strategy, skip this step.

- b. Upgrade the IDOL content (required fields).
- c. Upgrade the IDOL software.

After you start the program you can save progress so you can resume from the same step in the future.

NOTE: The program automates much of the upgrade process but you must update the IDOL software manually when prompted.

2. When the program completes, if IDOL is enabled with HTTPS in your environment, do the following:

- a. Open the \Install\Program Files\Micro Focus\ControlPoint\Engine\Scheduler\ControlPointConfiguration.exe.config file in a text editor.
- b. In the <appSettings> section, set the SecurePorts value to true:

```
<appSettings>  
  <add key="SecurePorts" value="true"/>  
</appSettings>
```

- c. Save the file.

3. If your environment has multi-layer IDOL DIH/DAH, do the following:

- a. Open the ControlPointIDOL Upgrade.exe.config file in a text editor.
- b. Edit the settings to reference the machine and correct port for the top-layer IDOL proxy.
- c. Save the file.

Complete the IDOL software upgrade manually

When the ControlPoint IDOL Upgrade program has finished, update the IDOL software manually.

To manually update the IDOL software

1. Stop the IDOL services.

To do so, as the local administrator, run the `_stop_services.bat` batch file generated by the IDOL Deploy Tool. This batch file is available at `\temp\ControlPoint\host_hostName`.

NOTE: If IDOL is running with HTTPS, stop IDOL services from Services and Processes manually.

2. Uninstall existing services by running `_uninstall_services.bat` as the local administrator.

Executing the file that was built for your current deployment will ensure spurious errors are not reported.

3. Prepare a new IDOL deployment using the **ControlPoint IDOL Deploy Tool** from the release media.

NOTE: To ensure your IDOL data migrates correctly, use the same Host Installation Directory as your current deployment:

Program Files*<companyName>*\ControlPoint

Where *<companyName>* is one of the following, depending on your current version of ControlPoint software:

Autonomy, Hewlett Packard, Hewlett Packard Enterprise, or Micro Focus.

The deployment is prepared.

4. Do the following:
 - a. Manually replace the `INSTALLATION_PATH\ControlPoint\Comms\jre` folder with a copy of the `temp\ControlPoint\host_<hostName>\Comms\jre` folder.
 - b. Manually copy `HP.HPTRIM.SDK.dll` and `HP.HPTRIM.SDK.xml` from `Program Files\Micro Focus\Content Manager` to `temp\ControlPoint\host_<hostName>\Indexer\Content Manager Connector`.
5. As the local administrator, run the `_deploy_services.bat` file and choose to overwrite all files.
6. As the local administrator, run the `_install_services.bat` batch file.

The new services are installed.

Update configuration files

This section provides information about how to update the configuration files that the upgrade process installs. To reuse custom values from the previous versions of these files, you must port those settings to the new files.

Update configuration files for DocKey update

If you [performed the DocKey update](#) after upgrading the ControlPoint database, complete the DocKey update process.

To update configuration files for the DocKey update

- Update the following configuration files:
 - ControlPoint\Dashboard\Web.config
 - ControlPoint\Engine\Scheduler\ControlPointTimer.exe.config
 - ControlPoint\LicenseService\ControlPointLicenseService.exe.config
 - ControlPoint\WebService\Web.config

by adding the following line to the end of the [appSettings] section in each file:

```
<add key="IgnoreCaseOnReferenceHash" value="false" />
```

Update Connector configuration files

Update the new Connector and Connector framework configuration files with specific configurations from your previous deployment.

The new files are located in component-specific subfolders under Program Files\Microsoft Focus\ControlPoint\Indexer. The previous versions of these files, which contain the values to port, are located in the backup copy of this folder you created while preparing your environment for upgrade.

To update Connector configuration files

1. Update the new versions of the following configuration files with values from your previous deployment:

- **Contents configuration files.** Make the following changes:
 - Port the [Databases] section from your backup copy. For example:

```
[Databases]
NUMDBS=4
0=News
1=Archive
2=FS
3=SPS
```
 - Port the [Repositories] section, located new the end of the file.

NOTE: Starting with ControlPoint 5.6.1, the IDOL Content configuration file contains only an entry for English in the [LanguageTypes] section. To support other languages, identify the languages you need and update the Content configuration file accordingly. For more information, see the IDOL documentation or contact Support.

- **IDOL configuration files.** Port details of all virtual databases, both the count and each vdb section. New vdb sections are typically added at the end of the file.

For example:

```
VirtualDatabases=4
[vdb2]
dbname=FS
type=combinator
mapsto=0:FS
[vdb3]
type=combinator
mapsto=0:SPS
```

- **SharePoint Remote configuration files.** In the DistributedConnector section, port the value of the ConnectorGroup parameter.
- **All connector configuration files.** Port every Task section.

For example:

```
[TaskFS]
DirectoryRecursive=True
ExtractOwner=True
PathRegex=.*
DirectoryFileAttributeFilter=-1
IngestActions=META:ENFORCESECURITY=false,META:CPREPOSITORYTYPEID=3,LUA:lua\ExtractFileData.lua,META:AUTN_CATEGORIZE=false,META:AUTN_EDUCTION=false
DirectoryPathCSVs=\\v-cptrim\FS
ScheduleStartTime=now
ScheduleCycles=1
ScheduleRepeatSecs=3600
IndexDatabase=FS
```

- **Some connector configuration files (such as SharePoint and Content Manager Connector),** additionally port all Groups task sections.

For example:

```
[Groups_TaskSPS]
FetchMode=0
IncludeEmptyFields=True
ExtractSubfiles=True
MappedWebApplicationPolicies=True
IgnorePublishingPagesAspx=True
SecurityType=SharePointSecurity
IngestActions=META:CPREPOSITORYTYPEID=2,META:AUTN_NO_FILTER=true
StartURL=http://v-cptrim:8081
ScheduleStartTime=now
ScheduleCycles=1
ScheduleRepeatSecs=3600
IndexDatabase=SPS
```

By default, ControlPoint 5.9.0 takes care of index synchronization. Therefore, you do not need to include entries for each task section in the [FetchTasks] section:

```
[FetchTasks]
Number=0
SynchronizeGroupsnnn=Groups_Taskxxxx
where nnn represents the incremental number from the last line and xxxx is
the name of the repository
```

After completion of the above task, increase the total number as shown:

```
SynchronizeGroupsNumber=totalNumber
```

NOTE: Ensure that the task configuration of each connector matches the configuration used in the previous deployment to prevent re-scanning of previously analyzed content.

- **All connector framework configuration files.** Port each Education settings section.

For example:

```
[FEducationSettings]
SearchFields=DRECONTENT
Entity0=number/ssdh/us
EntityField0=CPED_NUMBER_SS_US
Entity1=number/ssds/us
EntityField1=CPED_NUMBER_SS_US
Entity2=number/ssdn/us
EntityField2=CPED_NUMBER_SS_US
Entity3=number/ss/us
EntityField3=CPED_NUMBER_SS_US
Entity4=number/medicareid/us
EntityField4=CPED_NUMBER_SS_US
ResourceFiles=education\number_ss_us.ecr
```

2. **Connector Framework.** Port any custom LUA added after installation, along with any corresponding [ImportTasks] section entries.

NOTE: If you install a new version of ControlPoint in an installation directory which is different from the previous installation directory, then ensure you place the backed up categories directory in the new path.

3. **SharePoint2007, 2010, and 2013.** For new installations, only the SharePoint Remote connector type is supported. However, for upgrades, you can retain existing connector configuration files for the SharePoint versions listed. To do so, edit the appropriate SharePoint connector configuration files as follows:

- a. Add the following section anywhere in the file:

```
[Education]
DefaultMaxMatchesPerDoc=10000
```

- b. Update the [ImportTasks] section to contain the following lines:

```
Post2=lua:lua/Eduction.lua  
Post3=lua:lua/MetadataProvider.lua  
Post4=lua:lua/IndexingTarget.lua  
Post5=lua:lua/CFSFixup.lua  
Post6=lua:lua/Category.lua
```

- c. Update the [MyIdolIndexer] section to append the following line after last entry in section:

```
ACIPort=9070
```

- d. Update [Categorizer] section to append the following line after last entry in section:

```
ACIPort=9020
```

Update Insert Configuration files

If your environment contains Insert Configurations, update the Insert Configuration files by replacing them with those from your previous deployment.

The new files are located in component-specific subfolders under Program Files\Micro Focus\ControlPoint\Indexer. The previous versions of these files, which contain the values to port, are located in the backup copy of this folder you created while preparing your environment for upgrade.

To update Insert Configuration files

1. Replace the Program Files\Micro Focus\ControlPoint\InsertConfig folder with the backup copy of that folder you created while preparing your environment for upgrade.
2. Ensure that insert configurations are enabled by verifying that the InsertConfigEnabled parameter in the <AppSettings> section of the following file is set to **true**:

```
Program Files\Micro  
Focus\ControlPoint\Engine\Scheduler\ControlPointTimer.exe.config
```

Update Insert Configurations for Content Manager connectors

If needed, update the Content Manager insert configuration file with the custom insert configuration from your existing environment.

NOTE: Starting with version 5.9.0, the Content Manager connector uses the Content_Manager_Connector folder for the insert configuration. Therefore, you must port any previous Insert Configurations to it by updating them.

To update Insert Configurations for Content Manager connectors

1. On the **Administration** tab of ControlPoint Console, go to the Insert Configurations page.
2. In the **CONNECTOR GROUP** list, select Content Manager.

3. In the **FIELD MAPPING** section, recreate all the Content Manager custom field mappings you need.

For each mapping, do the following:

- a. In **Source Field**, enter or select the appropriate Content Manager-related field name.
- b. In **Target Name** and **Metadata Type**, enter the appropriate values to recreate your previous mappings.

For more information on Insert Configurations, see the ControlPoint *Administration Guide* (available from the [Micro Focus ControlPoint documentation site](#)) or the ControlPoint Help Center.

Update IDOL files (new IDOL locations only)

If while upgrading IDOL you changed its location, such as if you installed it on a different drive, you must manually copy some files from the previous installation so it can continue to access them:

- **Statistics .db files.** Copying these files from the previous version prevents IDOL from re-analyzing your repositories.
- **IDOL Category subfolders.** Copying these subfolders (`category`, `cluster`, `imex` and `taxonomy`) ensures that you can view your existing categories.

The previous versions of these items are located in the backup copy you created while preparing your environment for upgrade.

To update IDOL files

1. Copy all .db files from the following folders in your backup copy of `Indexer\Statistics` to the corresponding ones in `Program Files\Micro Focus\ControlPoint\Indexer\Statistics` of your new IDOL installation:
 - `dynterm`
 - `indexqueuepath`
 - `main`
 - `modules`
 - `nodetable`
 - `numeric`
 - `refindex`
 - `secindex`
 - `tagindex`

While copying files, overwrite any that exist in the new location.

2. Replace the following folders in `Program Files\Micro Focus\ControlPoint\Indexer\IDOL\category` of your new IDOL installation with the corresponding ones from your backup copy of `Indexer\IDOL\category`:

- category
- cluster
- imex
- taxonomy

Reconfigure the Documentum connector

If you deployed the Documentum connector, there are a few additional configurations to perform before using it.

Before you begin

Ensure you have the set of .Jar files that the Documentum connector requires. This task requires you to copy them into a specific folder.

NOTE: ControlPoint does not provide these files. For information or help obtaining these files, contact the Documentum Support team.

To configure the Documentum connector

1. In a text editor, update the Program Files\Micro Focus\ControlPoint\Indexer\Documentum Connector\dfc.properties file to include your Documentum server's host and port:

```
dfc.docbroker.host[0]=DocumentumHostName  
dfc.docbroker.port[0]=DocumentumPort
```

2. Copy the dfc.properties and dfc.keystore files from:

Program Files\Micro Focus\ControlPoint\Indexer\Documentum Connector

to the following two locations:

- Program Files\Micro Focus\ControlPoint\Indexer\OGS
- Program Files\Micro Focus\ControlPoint\Commons\dfc

3. Add the .Jar files required by the Documentum connector to the Program Files\Micro Focus\ControlPoint\Commons\dfc folder.

Perform post-upgrade steps

After the software upgrade completes, perform the following tasks:

1. Start the following services, in the specified order:
 - ControlPoint License Server
 - ControlPoint Content Engines
 - ControlPoint DataAnalysis Store

- ControlPoint OGS
 - ControlPoint IDOL
 - ControlPoint MetaStore
2. If you are installing ControlPoint in a directory other than your previous installation directory, copy all `connector_repositoryname_datastore.db` files to the new installation directory.
 3. When IDOL starts successfully, issue a **GETSTATUS** command to verify that all services are running and that all IDOL databases that were available before the upgrade are present.

For HTTP: `http://IDOLServerName:9000/a=getstatus`

For HTTPS: `https://IDOLServerName:9000/a=getstatus`

NOTE: If one or more expected IDOL databases are not present, do not proceed to the next step before resolving the problem.

4. When the MetaStore service successfully starts, issue a **GETSTATUS** command to verify that all services are running and that all MetaStore databases (which were available before the upgrade) are present.

`http://MetaStoreServerName:4500/a=getstatus`

NOTE: If one or more expected MetaStore databases are not present, do not proceed to the next step before resolving the problem.

5. Start the connectors in the following order:
 - a. Distributed Connector
 - b. Connector Framework Services
 - c. Connectors

CAUTION: Do not start the ControlPoint Engine until the full upgrade process completes.

6. If upgrading from a version of ControlPoint prior to 5.9.0 for the first time, use the ControlPoint Console to configure new required connector fields for all policies that have a Declare in Place action, as follows:
 - a. On the **Policy** tab, locate a card for a policy that has a Declare in Place action, click , and then click **Edit**.
 - b. In the policy's **Phases** field, click .
 - c. In the Policy Phase dialog box, set the following fields:
 - **Content Manager Document Store Name:** Specify the case-sensitive name of the document store. You can find the name as follows:
 - i. Open the Content Manager client.
 - ii. On the **Administration** tab, click **Document Stores**.

- iii. In the list of document stores, locate the name of the one with a **Type** of **Manage in Place** and whose **Configuration Information** contains information to the corresponding SharePoint connector, such as the URL to it.

TIP: To view **Configuration Information** for a particular document store, double-click the item's name to open the Document Store dialog box. The **Configuration Information** field is on the **Manage in Place** tab.

- **Content Manager Record Type:** Specify the case-sensitive record type. To determine this value:
 - i. On the **Administration** tab of the Content Manager client, in the **Search for** list, click **Origins**.
 - ii. In the list of origins, open the one that matches the **Origin Name** specified in ControlPoint for the policy's target.
 - iii. In the Origin dialog box, click **Defaults**, and locate the **Record Type** value.
- d. Click **Add**, and then click **Save**.

For more information on editing policies, see the *ControlPoint Administration Guide* (available from the [Micro Focus ControlPoint documentation site](#)) or the ControlPoint Help Center.

7. Enable scheduled tasks.
8. To view previously updated repositories in the ControlPoint Dashboard, clear your browser cache, restart the browser, and then navigate to the repositories.

For specific details on clearing the cache for your browser, see your browser's documentation.

9. If you performed the DockKey update after upgrading the ControlPoint database, perform a full re-scan on all Exchange repositories.

Rescan repositories having custom properties

IMPORTANT: This procedure applies only when upgrading to a ControlPoint environment in which you have *not* performed the database conversions documented in the *ControlPoint Database Conversion Guide*.

Skip this section if you have already converted your databases using the database conversion scripts provided with the ControlPoint software. For more information, see [Consider ControlPoint database partitioning and file groups, on page 99](#) and the *ControlPoint Database Conversion Guide*, available from the [Micro Focus ControlPoint documentation site](#).

If your ControlPoint environment has been configured with custom properties in repositories, additional steps are required after upgrading to 5.9.0.

For more reference material on configuring MetaStore for metadata ingestion, see [Metadata ingestion, on page 140](#) or the *ControlPoint Administration Guide* and ControlPoint Help Center.

To support custom property mapping after upgrade

1. In SQL Server, configure data mapping using the `MetaStore.MapField` stored procedure.
In this example, `AU_DOCUMENT_EDITOR_STRING` is the custom field that requires configuration.

```
USE ControlPointMetaStore
GO
EXEC MetaStore.MapField
@SourceName          = 'AU_DOCUMENT_EDITOR_STRING',
@TargetTable         = 'ControlPointMetadata.Additional',
@TargetColumn        = 'LastEditedBy',
@TargetTransform     = 'ToString'
GO
```

2. Refresh document ingest, import and update sequences to support the mapped field in `MetaStore`.

```
USE ControlPointMetaStore
GO
EXEC MetaStore.ConfigureAddDocument
EXEC MetaStore.ConfigureUpdateDocument
EXEC ControlPointMetadata.ConfigureImportDocument
GO
```

3. Restart the `MetaStore` service to utilize the refreshed sequences.
4. Rescan the repositories using the ControlPoint Dashboard.

Upgrade the ControlPoint Edge File System Connector

NOTE: Skip this step if you do not have ControlPoint Edge File System connectors in your environment.

To upgrade the ControlPoint Edge File System Connector

1. Back up the `Micro Focus\ControlPoint\Edge` folder.
Keep the original folder so the upgraded connector uses your existing `.db` files, which the next step does not uninstall.
2. Uninstall the ControlPoint Edge File System Connector and ControlPoint Edge Archive Service through Windows **Add/Remove Programs**.
3. Install the new version of the ControlPoint Edge File System Connector and Archive Service, and then restart the system.

For more information, see [Install ControlPoint Edge File System Connector software, on page 57](#).

4. After the system restarts, use Window Services to stop the ControlPoint Edge File System Connector and ControlPoint Edge File System Connector Framework services.
5. Open `ControlPoint Edge File System Connector.cfg` in a text editor, add the `TaskRepositoryName` and `PolicyTaskRepositoryName` sections from the back copy, and then save the file.
6. Open `ControlPoint Edge File System Connector Framework.cfg` in a text editor, add the `RepositoryNameEducationSettings` section from the back copy, and then save the file.
7. Use Window Services to start the ControlPoint Edge File System Connector and ControlPoint Edge File System Connector Framework services.

Configure the ControlPoint Edge File System Connector for HTTPS

The ControlPoint Edge File System Connector configuration file for Windows contains the following "EnableSSL" config section, which is disabled by default.

```
[EnableSSL]
SSLEnabled=false
```

If IDOL on the ControlPoint server is already using HTTPS, you should set `SSLEnabled` to `true` so the ControlPoint Edge File System Connector appears in the connection list on the Repository page of the ControlPoint Dashboard.

All other HTTPS configurations to run the ControlPoint Edge File System Connector on HTTPS are similar to the configuration of a regular File System connector.

Upgrade NiFi IDOL Ingest libraries

If you previously installed NiFi IDOL Ingest libraries, update to version 12.6.0, which is provided with ControlPoint 5.9.0.

To upgrade the NiFi IDOL Ingest libraries

1. Ensure that ControlPoint has finished ingesting all data and there is no data left in any ingestion pipeline.
2. Open the Apache NiFi UI in a browser using the following URL:
`https://NiFiInstallHost:port/nifi/`
Where `NiFiInstallHost` is the host on which your Apache NiFi installation resides.
3. Disable each NiFi processor by right-clicking it, and then clicking **Disable**.

4. Disable all NiFi controller services, as follows:
 - a. Click an empty space on canvas. On the left side of the canvas, click , and then click .
The **NiFi Flow Configuration** dialog box appears.
 - b. On the **CONTROLLER SERVICES** tab, disable each controller service by clicking  in the far-right column.

5. Stop the Apache NiFi service.
6. Delete the existing IDOL NiFi libraries (`idol-nifi-*.nar`) from the `NiFiInstallDir\lib` folder, which is where your Apache NiFi installation resides.
7. Copy the following NiFi libraries located in `ControlPoint\5.9.0\NiFiIngest` to the `NiFiInstallDir\lib` folder:

- `idol-nifi-framework-nar-12.6.0.nar`
- `idol-nifi-framework-api-nar-12.6.0.nar`

For detailed information about installing or using NiFi Ingest components, which run within Apache NiFi, see the NiFi Ingest help. To access the help, go to the [Micro Focus IDOL documentation web page](#), select IDOL version 12.6.0, and then click **NiFi Ingest** in the Connectors section of that page.

8. For each IDOL connector you use, copy its IDOL connector library (`idol-nifi-connector-connectorType-nar-12.6.0.nar` file) from the IDOL Deploy Tool's temp folder to `NiFiInstallDir\lib` folder.

For example, if you use the FileSystem connector, copy `C:\temp\ControlPoint\myServer\Indexer\FileSystem Connector\nifi\idol-nifi-connector-fileSystem-nar-12.6.0.nar` to `NiFiInstallDir\lib`.

9. Start the Apache NiFi service.
10. Open the Apache NiFi UI in a browser.
11. If you deployed any new types of connectors in step 8, add corresponding **GetConnectorType** processors.

For example, if you added a OneDrive connector, add a **GetOneDrive** processor.

To create **GetOneDrive** processors:

- a. Double click the **Config** process group, which opens a blank canvas.
- b. Add a **GetConnectorType** processor for each new connector type, and keep the default names.

To add a processor:

- i. On the toolbar click , and drag it to the canvas. The **Add Processor** dialog box opens.
- ii. In the **Type** column, double-click the name (**GetConnectorType**) of the processor to add. The dialog box closes and the new processor appears.

12. Enable all NiFi controller services, as follows:
 - a. Click an empty space on canvas. On the left side of the canvas, click , and then click .
The **NiFi Flow Configuration** dialog box appears.
 - b. On the **CONTROLLER SERVICES** tab, enable each controller service by clicking  in the far-right column.
13. Enable each NiFi processor by right-clicking it, clicking **Enable**, and then right-clicking it again and clicking **Start**.

Chapter 14: Configure Advanced IDOL Distribution

This chapter describes how to configure ControlPoint 5.9.0 for Advanced IDOL Distribution. You can perform this optional task after upgrading from a previous version that is not already configured for Advanced IDOL Distribution.

NOTE: Micro Focus recommends the Basic Distribution mode for most deployments. Advanced Distribution is beneficial only for very large environments. Using Advanced Distribution mode requires additional planning, installation steps, and resources. We recommend that you contact support if you want to use Advanced Distribution mode.

Basic Distribution mode is no longer deprecated and ControlPoint 5.9.1 and later do not enable Advanced mode by default.

IMPORTANT: The use of Advanced IDOL Distribution results in underlying data changes that are irreversible. Once enabled and ControlPoint restarts, you cannot disable this feature.

If you encounter a script error during this task, contact Micro Focus Support before proceeding to the next step.

To configure Advanced IDOL Distribution:

1. Ensure there are no outstanding ingestions or other connector-related activity in progress.
 - **Ingestions**
 - View queued ingestions:
`http://localhost:7200/a=QueueInfo&QueueAction=GetStatus&QueueName=Fetch&state=queued`
 - View active ingestions:
`http://localhost:7200/a=QueueInfo&QueueAction=GetStatus&QueueName=Fetch&state=running`
 - Stop scheduled ingestions:
`http://localhost:7200/action=PauseSchedules&Sections=MyTask,AnotherTask`
 - **Policies**
 - Check the `[ControlPoint].[dbo].[CPExecutionLog]` table to ensure that no policies are in progress.
2. Use Window Services to manually stop the following:
 - All Connector services
 - Connector Framework services

- MetaStore service
- ControlPoint Engine service

3. Open SQL Server Management Studio, and complete the following steps:

- a. Create a temporary folder for the script to use, such as C:\tmp.
- b. Ensure both the current Windows user account and the SQL Server service account (by default, NT Service\MSSQLSERVER) have full access rights to the temporary folder.
- c. Run the "1. updateReferenceHash.sql" script.

All SQL and PowerShell scripts required for this task are located in the ControlPoint\5.9.0\Utilities\Advanced IDOL Distribution Upgrade Scripts folder.

4. Export all IDOL data by Repo Name (IDOL database name) into separate folders:

- a. Create a folder on the local computer to hold the exported data and log files this task will create. For example: C:\IDXExport

Ensure the current user has full access rights to this folder. Exported data will be placed into subfolders specific to each repository. For example:

C:\IDXExport\RepoName1, C:\IDXExport\RepoName2, and so on.

- b. Open the "2. Export_IDX_ByRepoName.ps1" script in a text editor and set the following:

- **IdolHost:** List of Content Engine hosts. For example:

```
$IdolHost = @("hostname1", "hostname2");
```

- **IdolPort:** List of Content Engine Index ports on each host. The default port is 32001. For example:

```
$IdolPort = @("11001", "12001", "13001");
```

- **LogOutputPath:** Full path of the log folder you created in the previous step.

- c. Open the "2.1 ThreadedExport.ps1" script in a text editor and set the following:

- **MaxThreads:** Maximum number of concurrent threads for this script to use. The default is five threads.

- **IdolRepoNames:** List of all IDOL databases associated with ControlPoint repositories. For example:

```
$IdolRepoNames = @("Repo1", "Repo2", "Repo3")
```

You can identify the databases using the following command:

```
http://hostname:32000/a=getstatus
```

- d. Open PowerShell, and then run the "2.1 ThreadedExport.ps1" script.

NOTE: Check Indexer Status to ensure the export tasks are complete before moving to the next step. To do so:

- i. Go to `http://ContentEngineHostname:32000/a=admin`
- ii. Click **Monitor > Indexer Status**.
- iii. Ensure the **Status** column indicates all tasks have finished.

5. Use Window Services to manually stop the following:

- IDOL services
- ControlPoint Content services

6. Update the IDOL configuration file to include a new central IDOL database, such as one named ContentRepo.

NOTE: Examples in this task use ContentRepo as the database name.

- a. Open the `C:\Program Files\Micro Focus\ControlPoint\Indexer\IDOL\ControlPoint IDOL.cfg` file in a text editor.
- b. Locate the `VirtualDatabases` section and complete the following steps:
 - i. Delete any existing virtual database sections under it other than `Archive` and `News`—keep only those two sections.
 - ii. Add a virtual database section that maps to the new database.
 - iii. Set `VirtualDatabases=3`

For example:

```
VirtualDatabases=3 <--set to "3"
```

```
[vdb0]
```

```
DbName=News
```

```
Internal=False
```

```
Type=combinator
```

```
MapsTo=0:News
```

```
[vdb1]
```

```
DbName=Archive
```

```
Internal=False
```

```
Type=combinator
```

```
MapsTo=0:Archive
```

```
[vdb2] <--add
```

```
DbName=ContentRepo
```

```
Internal=False
```

```
Type=combinator
```

```
MapsTo=0:ContentRepo
```

c. Save the file.

7. Add the new IDOL database to the content engine configuration file.

- a. Open the `C:\Program Files\Micro Focus\ControlPoint\Indexer\Content\ControlPoint Content.cfg` file in a text editor.

- b. In the `SetDatabaseFields` section, update the line shown in bold:

```
[SetDatabaseFields]
Property=DatabaseFields
PropertyFieldCSVs=*/DREIDOLDBNAME
```

- c. Locate the `[Databases]` section and complete the following steps:

- i. Delete any existing IDOL database entries other than `News` and `Archive`—keep only those two.
- ii. If you deleted any items, delete their corresponding section, which appears after the `[Databases]` section.

For example, if from the `[Databases]` section you delete the entry `2=MyIdo1DB`, also delete the corresponding `[MyIdo1DB]` section.

- iii. Add a database-specific section for the new database.
- iv. In the `[Databases]` section, set `NUMDBS=3`.

For example:

```
[Databases]
NUMDBS=3 <--set to "3"
0=News
1=Archive
2=ContentRepo <--add

[ContentRepo] <--add
```

- d. Save the file.
8. In non-proxy based configurations only, remove existing IDOL databases from each `DAH.cfg` file and add the new one, as described in steps 7c and 7d.
9. For the following components, delete the subfolders listed:

- **Indexer\Content**

- Default location: `C:\Program Files\Micro Focus\ControlPoint\`
- Delete: `actions`, `bitfield`, `dynterm`, `indextmp`, `logs`, `main`, `nodetable`, `numeric`, `reindex`, `secindex`, `sortfield`, `status`, `storedstate`, and `tagindex`

- **IDOL\DAH**

- Default location: `C:\Program Files\Micro Focus\ControlPoint\Indexer\IDOL\dah`
- Delete: `logs`, `statetokens`, and `status`

- **IDOL\DIH**

- Default location: `C:\Program Files\Micro Focus\ControlPoint\Indexer\IDOL\dih`
- Delete: `archive`, `failed`, `incoming`, `logs`, and `main`

NOTE: If your environment contains multiple DAH or DIH components, delete the subfolders from each component location.

10. Update all Connector configuration files in your environment with the new IDOL database:
 - a. Create a temporary folder on the local computer and copy all Connector configuration files to it.

For example:

```
C:\CP_AdvIDOLDistrib\ConnectorCFGs
```


Having all configuration files in one folder enables a script you run to easily update them.
 - b. Open the "3. UpdateConnectorCFGs.ps1" script in a text editor, and set the following:
 - i. **FolderPathWin**: Full path of the folder you created in the previous step.
 - ii. **MoveFromNonAdvancedMode**: If upgrading from Standard to Advanced IDOL distribution, set to \$TRUE. Otherwise, set to \$FALSE.
 - iii. **IdolRepoNames**: List of all IDOL databases associated with ControlPoint repositories.
 - iv. **IDOLDBName**: The name of the new single IDOL database, such as **ContentRepo**.
 - v. (Optional) **BackupOriginal**: To create backups of the Connector configuration files in **FolderPathWin** before updating them, set to \$TRUE. Otherwise, set to \$FALSE.
 - vi. (Optional) **importedPath**: If **BackupOriginal** is set to \$TRUE, specify a folder to hold backup copies of the configuration files. For example:

```
[string] $importedPath = (".\backupOriginal\")
```
 - c. Open PowerShell, and then run the "3. UpdateConnectorCFGs.ps1" script.
 - d. Copy the updated Connector configuration files from **FolderPathWin** back to their original locations.

11. Using a text editor, update each CFS configuration file:
 - a. Add `ModifyReference.lua` to the end of the `[ImportTasks]` section.
 - b. Move the existing `Eduction.lua` section after the new `ModifyReference.lua` section.

For example, an `[ImportTasks]` section that contains the following:

```
Post2=lua:lua/Eduction.lua
Post3=lua:lua/MetadataProvider.lua
Post4=lua:lua/IndexingTarget.lua
Post5=lua:lua/CFSFixup.lua
Post6=lua:lua/Category.lua
```

Results in the following:

```
Post2=lua:lua/MetadataProvider.lua    <--renumbered
Post3=lua:lua/IndexingTarget.lua
Post4=lua:lua/CFSFixup.lua
Post5=lua:lua/Category.lua
Post6=lua:lua/ModifyReference.lua    <--added
Post7=lua:lua/Eduction.lua    <--moved from beginning
```

12. If upgrading from a ControlPoint 5.6.1 environment that has Advanced IDOL mode configured, disable it.

To do so, open SQL Server Management Studio, and then run the "6.disableAdvancedMode.sql" script.

13. Launch ControlPoint Configuration Manager and do the following on the **IDOL** settings tab:
 - a. Click **Enable Advanced IDOL Distribution**.
 - b. In the **Advanced IDOL Distribution Database** field, enter the name of the IDOL database name that you specified on the **IDOL** tab of the IDOL Deploy Tool while configuring the deployment packages.

For example: ContentRepo

14. Use Windows Services to start the following:

- All Connector services
- Connector Framework services
- IDOL services
- ControlPoint Content services
- MetaStore service
- ControlPoint Engine service

NOTE: Verify that all services have started.

15. Run the IDOL database's update and import script:

- a. Create a folder on the local computer to hold the logs this script creates.
- b. Open the "4. UpdateAndImportIDX.ps1" script in a text editor, and set the following:
 - **FolderPathWin:** Full path of the folder that contains the exported repository data. This is the folder you created in step 4a and assigned to **LogOutputPath** in step 4b. For example:

```
[string] $FolderPathWin = "C:\IDXExport\"
```
 - **IdolHost:** IDOL Data Indexer (DIH) host.
 - **IdolPort:** DIH Index port. The default port is 9071.
 - **IdolACIPort:** DIH ACI port. The default port is 9070.

- **IDOLDBName:** Name of the new single IDOL database, **ContentRepo**.
 - **LogPath:** Full path of the log folder you created in the previous step in which the script will create `QueryResults_Import_repoName.txt` to hold the Index IDs it imports to DIH.
 - **LogOutputPath:** Full path of the log folder you created in the previous step in which the script logs any failures to `UpdateAndImportIDX_repoName.log`.
- c. Open the "4.1 ThreadedImport.ps1" script in a text editor, and set the following:
- **IdolRepoNames:** List of all IDOL databases associated with ControlPoint repositories. For example:

```
$IdolRepoNames = @("Repo1", "Repo2", "Repo3")
```

You can identify the databases using the following command:

```
http://hostname:32000/a=getstatus
```
- d. Open PowerShell, and then run the "4.1 ThreadedImport.ps1" script.
16. Run the categories migration script:
- a. Create a folder on the local computer to hold the logs this script creates, such as `C:\tmp\`. Ensure the current Windows user account has full access rights to this location.
- b. Open the "5.MigrateCategories.ps1" script in a text editor, and set the following:
- **IdolHost:** IDOL Data Indexer (DIH) host.
 - **IdolPort:** DIH Index port. The default port is 9071.
 - **IDOLDBName:** Name of the new single IDOL database, **ContentRepo**.
 - **OutputPath:** Full path of the folder created in the previous step in which the script logs category migration status.
- c. Open PowerShell, and then run the "5.MigrateCategories.ps1" script.

Chapter 15: Troubleshooting

This section provides troubleshooting information on the following:

- [Connectors](#)
 - [Edge Filesystem connectors](#)
 - [SharePoint connectors](#)
 - [Content Manager connectors](#)
- [Compact stored procedure](#)
- [Diagnostics logs](#)
 - [Policy execution logs](#)
 - [Data Analysis logs](#)
 - [Statistics Export utility trace logs](#)
- [IDOL](#)
 - [Remote connectors](#)
 - [HTTPS setup for IDOL](#)
 - [IDOL distributed mirror / non-mirror setup](#)
- [Policy execution](#)
- [Proxy server interactions](#)

Connectors

KeyView import.log failure if File System connector framework account and share permissions are not sufficient

Symptom

For shares in certain secure Connector environments, files could not be viewed in the ControlPoint user interface.

The File System connector framework service `import.log` displayed failures in the IDOL KeyView subcomponent's ability to create temporary files and scan the share.

For example:

```
17/02/2017 10:42:19 [2] 70-Error: Failed to open KV stream: Unable to create temp
file [\\CR-WIN2008-61.swlab.net\FileShare2\Investigating network performance
issues.docx]
```

...

```
17/02/2017 10:42:19 [2] 70-Error: KV: FilterInterface.fpGetDocInfoFile() failed
```

Solution

- Ensure that the Connector Framework service and the Connector are configured to use the same service account.
- Ensure that the service account for the Connector and Connector Framework service has full rights to the Connector's share location.

CPCategory field is missing from the Advanced Properties during rescan of Connectors configured in SSL environments

Problem

When ControlPoint is enabled with SSL, you do not see CPCATEGORYTAG under the Advanced Properties of a document. Instead, you see CPDEFAULTCATEGORYTAG under IDOL Properties section in the Advanced Properties with the name of the parent category.

Scenario

The following scenario can exhibit the problem:

1. Create two content repositories with text (.txt) files.
2. Create a category, which is treated as the parent category.
3. Create another category under the parent with criteria for the file type .txt and use Repository 1 for training.
4. Edit Repository 2 and CP adds the Default category for the repository, as seen on the Analysis page, as the parent repository name.

Expected behavior

When a repository is assigned a category and a document satisfies a category criteria, the category name should be displayed for the CPCATEGORYTAG field in Advanced Properties.

Solution

The Category LUA file on the Connector Framework must be edited to include extra parameters for SSL communications in the environment.

To edit the LUA file on each Connector Framework

1. Navigate to the file location:

```
Program Files\Micro  
Focus\ControlPoint\Indexer\<connectorFramework>\lua\Category.lua
```

For example:

```
Program Files\Micro Focus\ControlPoint\Indexer\FileSystem Connector  
Framework\lua\Category.lua
```

2. Search for the line:

```
local categorize = document:getFieldValue("AUTN_CATEGORIZE",false)
```

3. Insert a new statement after the statement in step 2:

```
local sslParameters =  
{  
    SSLMethod = "TLSV1.2",  
}
```

4. Edit the line:

```
local xmlString = send_aci_action(hostName, port, "CategorySuggestFromText",  
{querytext = content, NumResults = maxCategories, textparse = "true",  
agentBoolean = "true", anylanguage = "true", FieldText = "NOT EXISTS  
{}:CONTAINERCAT AND NOT EXISTS{}:SHADOWCATEGORYOF"}, timeout, retries )
```

to

```
local xmlString = send_aci_action(hostName, port, "CategorySuggestFromText",  
{querytext = content, NumResults = maxCategories, textparse = "true",  
agentBoolean = "true", anylanguage = "true", FieldText = "NOT EXISTS  
{}:CONTAINERCAT AND NOT EXISTS{}:SHADOWCATEGORYOF"}, timeout, retries,  
sslParameters )
```

5. Save the file.

Stop and start the Connector services, in order:

1. Stop the Filesystem Connector service.
2. Stop and start the Filesystem Connector Framework service.
3. Start the Filesystem Connector service.

Temporary files accumulate in different locations when indexing repositories

Problem

When indexing repositories, temporary files can accumulate in different locations. This may impact performance, create out-of-disk conditions, or cause corruption in IDOL.

Symptoms

The following symptoms may occur:

- On Connectors, temporary files may accumulate in the Connector's \Temp directory.

For example, on a File System connector:

```
C:\Program Files\Micro Focus\ControlPoint\Indexer\FileSystem Connector\Temp
```

- In the operating system temporary files location, usually set in the environment variables, ControlPoint temporary files may accumulate.

For example, in Windows:

```
C:\Users\%serviceaccount%\AppData\Local\Temp
```

Solutions

For Connectors:

- Ensure that the Connector Framework service and the Connector are configured to use the same service account.
- Ensure that the service account for the Connector and Connector Framework service has full rights to the Connector's \Temp location.

For the operating system temporary location:

- Utilize all of the following parameters in all CFG framework files

```
[ImportService]
KeyviewTemporaryPath=<full path to CFS folder+specific folder>
KeyviewDirectory=<full path to CFS folder+specific folder>
WorkingDirectory=<full path to CFS folder+specific folder>
ExtractDirectory=<full path to CFS folder+specific folder>
```

where

- KeyviewTemporaryPath is the path KeyView uses for extraction.
- WorkingDirectory is the path where temporary files are extracted and then copied to the extracted directory when finished.
- ExtractDirectory is the path used for the extracted files, for example, email attachments or zip files.

NOTE: Temporary files are not deleted for particular KeyView processes if filtering fails. It may be related to particular files which need to be identified and analyzed in more detail.

To proceed with further investigations, set the following parameters and ensure that you have enough space, because the original files will be kept.

```
[ImportService]
KeepExtractedFiles=true
[Logging]
```

```
LogLevel=full
```

This test should be processed with clean temporary folders and logs. When the fetch cycle is complete, attach all logs and temporary folders for analysis.

ControlPoint MetaStore service shows sustained very high memory and CPU usage and the Connector Framework service shows very high CPU usage

Problem

The documents ingested by a Connector from the source repository are processed by a Connector Framework service that then forwards them in batches to the ControlPoint MetaStore service. The metadata associated with each document varies considerably depending on, for example, whether education grammars have been selected for the source repository and how many educed fields are discovered within each document. If the total size of data in each batch of documents the Connector Framework service sends to the ControlPoint MetaStore service is very large, it can affect the CPU and memory usage of both services.

Symptoms

During ingestion, the Connector Framework service shows periods of very high CPU usage and the ControlPoint MetaStore service shows sustained very high CPU and memory usage.

Solutions

To prevent the Connector Framework and ControlPoint MetaStore services from using an excessively high amount of CPU and memory when you know in advance that document batches are likely to be large, decrease the batch size. For example, if you plan to specify education grammars that will probably generate a lot of metadata for each document, then decrease the batch size. To do so, modify the `IndexBatchSize` setting in the `[Indexing]` section of the Connector Framework service configuration file. This setting controls the number of documents per batch. For example, the following configures a maximum batch size of 10 documents per batch:

```
[Indexing]  
IndexBatchSize=10
```

Edge Filesystem connectors

Unable to remove the DeleteArchive Policy once it is applied

Problem

After you edit the Edge Connector repository and remove the Archive Policy or DeleteArchive policy and rescan the repository, you will see that the removed policies are still in effect.

Solution

Remove the LuaCache.cache from the Edge Connector directory and then rescan.

SharePoint connectors

EncryptACLEntries=False does not work if it is in the [Connector] section.

Problem

EncryptACLEntries=False does not work if it is in the [Connector] section.

Affects

All SharePoint connectors.

Solution

The EncryptACLEntries parameter must be set in the [TaskName] section for the Sharepoint Connectors. If the parameter is in the [Connector]section, it will not work as expected.

Content Manager connectors

Insert into Content Manager fails when document title exceeds 128 characters

Symptom

Items whose titles exceed 128 characters fail to be ingested into Content Manager through a ControlPoint policy.

The policy logs may display error messages in the following manner:

```
30-Normal: FETHTASKS: Inserting 1 document
```

```
70-Error: Insert Failed": file specified for insertion doesn't exist.
```

Problem

This is a Windows limitation in the overall length of a file path plus file name.

When an insert into a Content Manager location is performed, two more levels of folders are appended to the file name by the ControlPoint connector software. In addition, the actual file name is prefixed with additional characters when it is inserted.

This causes long file names or file paths to exceed the Windows MAX_PATH=260 limitation.

Workaround

To work around this issue, create a new policy for the insert action and create a new policy-based temporary location using a shorter path.

For more information on creating a new policy with a policy-based temporary location, see the *ControlPoint Administration Guide* (available from the [Micro Focus ControlPoint documentation site](#)) or ControlPoint Help Center.

Compact stored procedure

The Compact stored procedure takes more than several days to complete

Problem

When a Compact stored procedure job does not complete before the next scheduled run, then both instances of Compact will run. This slows down the database performance and may prevent ingestion and other operations from running.

Scenario

In the ControlPointMetaStore database, the Compact stored procedure runs once a week, and its purpose is two-fold:

- To delete any deleted repositories and their associated document-related information which exist in several tables.
- To remove unused hashes for deleted documents as a result of incremental scans or policy executions.

Solution

The Compact stored procedure does the following:

- Prevents more than one Compact job from running at a time.
- Always delete all repositories that are marked for deletion.

- Performs cleanup of unused hashes on a limited number of repositories.

Two settings in the ControlPoint**MetaStore.Metadata.Settings** table control the Compact stored procedure. You can adjust these settings for your particular ControlPoint environment.

Setting Name	Description
Compact NoIngestTimeMins	The number of minutes of no ingestion activity to wait before unused hash cleanup runs. Default: 15 NOTE: This setting was hardcoded in previous releases.
CompactNumReposToCleanupUnusedHash	The maximum number of repositories to perform the cleanup of unused hashed cleanup on. Default: -1 (all repositories) NOTE: This setting was hardcoded in previous releases.

If you think the Compact stored procedure is stuck and has not finished running after one week, you can clear the **IsRunning** flag.

To clear the IsRunning flag, run the following SQL command

```
UPDATE [ControlPointMetaStore].[Metadata].[CompactLock] set IsRunning = 0
```

IMPORTANT: Use caution when deciding to clear the **IsRunning** flag. Ensure that you have waited long enough for the Compact operation to complete.

If you find that the Compact job is taking longer than several days to complete and is affecting the operation of your ControlPoint environment, adjust the Compact stored procedure settings.

To adjust the Compact stored procedure settings

- Set the **CompactNumReposToCleanupUnusedHash** to 25 percent of the number of repositories.

Example

For 100 repositories, set the CompactNumReposToCleanupUnusedHash to 25.

```
update [ControlPointMetaStore].[MetaStore].[Setting] SET Value=5  
where name='CompactNumReposToCleanupUnusedHash'
```

Diagnostics logs

This section provides information on the following diagnostics logs for ControlPoint.

Policy execution logs

As part of investigation and diagnostics of policy execution issues, you can change the logging level of the ControlPoint Engine. Logging levels can be changed with the Configuration Manager or by editing the configuration file.

To change the logging level with Configuration Manager

1. Open the ControlPoint Configuration Manager.
2. In the **Engine** section, click **Logging**.

The Logging tab opens.

3. Click **Execute Policies** and select a logging level setting from the **Log Level** list. The default level is Information. The available logging levels are:

- All

NOTE: Micro Focus recommends to set the logging level to **All** when your ControlPoint environment is encountering issues with policy execution. This level gathers the most diagnostic information.

- Verbose
- Information
- Warning
- Error
- Off

4. Click **Deploy**.

ControlPoint redeploys.

To change the logging level in the configuration file

1. Navigate to the `\Program Files\Micro Focus\ControlPoint\Engine\Scheduler\ControlPointTimer.exe.config` file.
2. Edit one of the following settings in the `<categorySources>` section of the configuration file to the desired logging level:

- `<add switchValue="Information" name="Execute Policies">`

This setting applies the logging level across all policy execution schedules.

For example:

```
<add switchValue="All" name="Execute Policies">
```

- `<add switchValue="Information" name="Execute Policies (High)">`
- `<add switchValue="Information" name="Execute Policies (Normal)">`
- `<add switchValue="Information" name="Execute Policies (Low)">`

The above three settings apply the logging level to each schedule frequency level individually.

3. Save the file.
4. Restart the **ControlPoint Engine** service.

The configuration changes take effect.

Data Analysis logs

Data Analysis Service and Data Analysis Controller logs have been improved so you can use them as part of investigation and diagnostics of Data Analysis issues.

Data Analysis service logs

Logs for the Data Analysis service can be found at the following location:

```
\Program Files\Micro Focus\ControlPoint\DataAnalysis\Service\Logs\Logs.log
```

NOTE: The Data Analysis service logs contain only errors.

Data Analysis Controller logs

Logs for the Data Analysis Controller have been improved for events for Analysis jobs.

- Error messages: For events such as OnFailed or OnIssues.
- Informational messages: For events such as OnProgressUpdate, OnJobComplete, OnJobCancelled, and so on.

Logs for the Data Analysis Controller can be found at the following location:

```
\Program Files\Micro Focus\ControlPoint\DataAnalysis\Controller\Logs\controller_<GUID>.log
```

Statistics Export utility trace logs

As part of investigation and diagnostics of Statistics Export issues, you can enable a System.Diagnostics trace log in the Statistics Export utility.

To enable trace logs

1. Edit the Statistics Export utility configuration file, which is available at the following location:

```
ControlPoint<version>\Utilities\Statistics Export  
Utility\ControlPointStatisticsUtility.exe.config
```

2. In the <Configuration> section, add the following parameters:

```
<!--  
System.diagnostics-- to be removed once problem is resolved  
-->  
  <system.diagnostics>  
    <trace autoflush="false" indentsize="4">  
      <listeners>  
        <add name="myListener" type="System.Diagnostics.TextWriterTraceListener"  
initializeData="TextWriterOutput.log" />  
        <remove name="Default" />  
      </listeners>  
    </trace>  
  </system.diagnostics>
```

3. Save the file.
4. Run the Statistics Export utility.

The utility runs with an increased level of logging.

IDOL

This section provides troubleshooting information for the IDOL components.

Remote connectors

Preview of items on remote connectors

Problem

In the Console, when you attempt to preview a document residing on a remote connector, the document is not displayed.

Scenario

By default, the IDOL component runs under the Local System identity. This works for files that reside on shares on the same system as the IDOL component.

However, when IDOL attempts to access a file in its physical location on a remote connector server, it will fail unless the computer account of the IDOL server is given permission to that share.

Solution

- Ensure that the IDOL components and the Connector services are configured to use the same service account.
- Ensure that the service account has full rights to the Connector's share location.

HTTPS setup for IDOL

Verify HTTPS setup for IDOL

Description

Verify that all the ports are up and running with HTTPS.

Solution

1. Modify the configuration files for connectors and IDOL with SSL settings.
2. Verify that all the ports are up and running with HTTPS. Run the following commands:
 - a. DC port : `https://localhost:7000/a=getstatus`
 - b. File system connector : `https://localhost:7200/a=getstatus`
 - c. IDOL port: `https://localhost:9000/a=getstatus`
 - i. Category DRE: `https://localhost:9020/a=getstatus`
 - ii. Community: `https://localhost:9030/a=getstatus`
 - iii. agentstore: `https://localhost:9050/a=getstatus`
 - iv. DAH: `https://localhost:9060/a=getstatus`
 - v. DIH : `https://localhost:9070/a=getstatus`

```
<engine>  
  <number>0</number>  
  <group>0</group>  
  <host>TestVM</host>  
  <port>32000</port>  
  <status>UP</status>  
  <updateonly>>false</updateonly>  
  <weight>1</weight>
```

```
        <disabled>false</disabled>  
    </engine>
```

- vi. Verify the status of the engine. It should be up and running.

View: `https://localhost:9080/a=getstatus`

3. Content Engine : `https://localhost:32000/a=getstatus`
4. DataAnalysis DataStore: `https://localhost:31500/a=getstatus`
5. Similarly, for other connectors that are installed, perform a check on the respective port numbers.

Port numbers can be found in the configuration file under the [Server] section.

Repository page does not list registered repositories after changing the IDOL setup on HTTPS

Problem

You have registered repositories, but after changing the IDOL setup on HTTPS, the repository page is not listing the registered repositories.

Description

This issue could happen in the following circumstances:

1. A caching issue in the browser.
2. A repository created with a connector, which is not configured with SSL settings. The repository page makes a call to `ListConnectors` and waits for all connectors with repositories to return.

Solutions

- Clear the browser cache and reload the page.
- Verify the SSL settings in the connector configuration file.

ControlPoint Configuration Manager cannot establish trust relationship

Problem

The ControlPoint Configuration Manager displays the following error message when you click **Deploy**.

```
Could not establish trust relationship for the SSL / TLS secure channel
```

Solution

1. Ensure that the CA certificate for IDOL is imported to the Trusted root authority certificate store on your local computer.

2. Double click the certificate file to verify the details of the Server certificate for IDOL.
3. Ensure that ControlPoint Configuration Manager has the same name as provided in the certificate on the host for DataAnalysis, IDOL server settings and for MetaStore.

IDOL distributed mirror / non-mirror setup

DAH stops working after the Content Engine stops running

Problem

DAH stops working after the Content Engine stops running.

Description

DAH requires at least one content engine to be running. If only one content engine is running and manages DAH, then DAH will not work after that content engine stops running. The health check does not check those components that are not configured in the IDOL proxy server configuration file.

Solution

NOTE: Micro Focus recommends that you set up more than one content engine under each second-tier DIH/DAH.

To temporarily resolve the issue

1. Check if there are any components under <components> that are not running.
`http://IDOL_PROXY_SERVER_HOST:9000/a=getstatus`
2. Verify the DIH status:
`http://STANDALONE_DIH_INSTALLATION_HOST:SERVER_PORT/a=getstatus`
3. Verify the DAH status:
`http://STANDALONE_DIH_INSTALLATION_HOST:SERVER_PORT/a=getstatus`
4. Verify the content engine status:
`http://CONTENT_ENGINE_HOST:SERVER_PORT/a=getstatus`
5. Locate the stopped content engine and start it.

Policy execution

This section describes some items for ControlPoint policy executions.

Documents remain at 'Executing' state

Problem

Residual locks in the ExecutionLog table caused by engine crashes can cause documents to be stuck in the 'Executing' state.

Solution

To enable the clearing of locks on the ExecutionLog table at Engine startup, enable the ClearLocksAtStartup option in the ControlPointtimer.exe.config file.

1. Navigate to the \Program Files\Microsoft Focus\ControlPoint\Engine\Scheduler\ControlPointTimer.exe.config file.
2. Open the file in a text editor and enable the ClearLocksAtStartup setting.
3. Save the file.

For more information on individual settings in ControlPointTimer.exe.config, see the appendixes in the *ControlPoint Best Practice Guide*.

4. Restart the ControlPoint Engine service.

Policy execution phase fails to acquire locks on any items

Problem

Items are stuck in the ExecutionLog table and the policy execution log shows the policy execution phase failed to acquire locks on any items.

Symptoms

The log displays No items to process in the trace logging mode.

Scenarios and solutions

Scenario	Solutions
To avoid overloading the connector, the engine stops sending more document actions to the connector if there are too many items in State 30 (pending callback) for each connector group.	You need to wait until the connector callback are processed.
Restarting the engine caused some locks to be left on certain items.	See Documents remain at 'Executing' state, above .
Erroneous GlobalSettings table settings.	For more information on global settings, see the <i>ControlPoint Best Practice Guide</i> ,

Scenario	Solutions
	available from the Micro Focus ControlPoint documentation site .

Delay in showing failed items as 'Failed' in the policy details page

Problem

There is a delay in showing failed items as Failed on the Policy Details page, even if the items in ExecutionLog table show 'items received issue' messages from the connector.

Explanation

This is not an issue and it is expected behavior.

The Process Issues scheduled task processes failed callbacks and shows the failed results in the UI and displays the issue message in the Issues Management page in the Administration Dashboard.

When you specify to abort or retry the issue, the scheduled task must run once before it will process your requests to retry or abort the issue.

If you specify to abort the policy execution for some documents, the documents will be unassigned from the policy.

If you specify to retry, after the scheduled task is run, the Execute Policies scheduled task will need to run to retry the policy execution for those documents.

Solution

The Process Issues scheduled task can be set to run in a higher frequency to avoid the delay.

Communications errors attempting to execute an action

Problem

The policy execution logs display one of several communications errors while attempting to execute an action:

- A communications error has occurred attempting to execute an action
- Unable to connect to the remote server

Solution

Verify that both the MetaStore and IDOL services are running. They need to be running for the policy execution engine to function.

Proxy server interactions

Proxy server blocks traffic of Data Analysis service

Problem

The system was routing all calls to the Data Analysis service through a proxy server, which was blocking certain calls.

Solution

1. Open the \Program Files\Micro Focus\ControlPoint\DataAnalysis\Service\web.config file.
2. Add the following section between the </system.web> and <system.ServiceModel> sections:

```
<system.net>  
  <defaultProxy>  
    <bypasslist>  
      <add address="1.2.3.4"/>  
      <add address="5.6.7.8"/>  
    </bypasslist>  
  </defaultProxy>  
</system.net>
```

3. Save the file.
4. Reset IIS to allow the environment to load the changes.

Chapter 16: Metadata ingestion

This section provides an overview of the steps necessary to configure ControlPointMetaStore to capture additional data during document ingestion. A set of examples will be used to show where and how this data can be captured.

- [Data mapping](#)
- [Additional data capture](#)
- [Examples](#)
 - [Example 1: Single value for the same document](#)
 - [Example 2: Single value hash for the same document](#)
 - [Example 3: Multiple values for the same document](#)
 - [Example 4: Multiple values hashed for the same document](#)
- [Existing data and re-ingestion](#)
- [Field text and advanced properties](#)

Data mapping

Document metadata is captured by a list of instructions dynamically generated based on information held in the **MetaStore.MapTable** and **MetaStore.MapColumn** tables.

A stored procedure named **MetaStore.MapField** handles the complexity of these mapping tables. Run this stored procedure to register data mappings for any additional document metadata to be captured into ControlPoint MetaStore.

MetaStore.MapColumn

Field	Description
GroupNumber	Used when a source field is mapped to multiple times the same target table. For example, use GroupNumber for a complex field such as "ADDRESS" with a value {CITY="Boston", NUMBER=10, STREET="Main"}. The inclusion of the same GroupNumber for the separate address parts keeps the information together within the one row in the target table. Default: 1
SourceName	The field to be extracted from the source document.

Field	Description
ExtractPath	The value of this field is typically null, except when a value is to be parsed from the source field.
TargetColumn	The name of the column where the captured value is to be stored.
TargetTransform	The type of transformation to be used before storing the captured value.
TargetTransformParams	When a transformation requires additional configuration, the configuration can be placed in the TargetTransformParams field. The value of this field is typically null.
SupportingTable	The name of the target hash table, if any. This field should be populated when the extracted data is to be hashed into a separate hash table.
CanUpdate	Indicates whether the information captured to the target column can be modified after creation.
Inherit	Indicates whether the information captured to the target column, when modified, should be captured to child documents. Examples of such inheritance would be security.
AlternativeFieldSource	The alternate field to be extracted from the source document when SourceName cannot be extracted.
AlternativeFieldSourceTransform	The alternate transform to be used when AlternativeFieldSource is specified.

MetaStore.MapTable

Field	Description
GroupNumber	See GroupNumber
SourceName	See SourceName
TargetType	The TargetType values are as follows: <ul style="list-style-type: none"> “MVF” if the table can capture multiple values for the same document. For example, more than one row can exist for a given document.

Field	Description
	<ul style="list-style-type: none"> “SVF” if the table can capture single values for the same document. For example, a maximum of one row can exist per document.
TargetTable	The name of the table to populate.
TargetMVPSuffix	<p>Supports the extraction of a suffix from the source field name to further populate a column in the target table.</p> <p>For example, assuming data exists in the source document like:</p> <pre>CPPATH1=\\c\ CPPATH2=\\c\test\ CPPATH3=\\c\test\folder\ </pre> <p>Then it is possible to map CPPATH* as the SourceName and indicate that the value extract from * should be placed in the field configured by TargetMVPSuffix, for example “Level”.</p>
TargetMVPSuffixTransform	Specifies the transform to use when extracting a suffix. See TargetMVPSuffix .

MetaStore.MapField

The stored procedure **MetaStore.MapField** handles the complexity of the mapping tables by defaulting a number of optional parameters to typical values.

Parameter Name	Required	Default Value
@GroupNumber	No	(1), defaults to a single field mapping
@SourceName	Yes	
@TargetType	No	('SVF') , defaulting Single-valued Field (SVF)
@TargetTable	Yes	
@TargetMVPSuffix	No	(NULL), defaults to not specified
@TargetMVPSuffixTransform	No	(NULL), defaults to not specified
@ExtractPath	No	(NULL), defaults to not specified
@TargetColumn	Yes	
@TargetTransform	Yes	
@TargetTransformParams	No	(NULL), defaults to not specified

Parameter Name	Required	Default Value
@SupportingTable	No	(NULL), defaults to not specified
@CanUpdate	No	(1) , defaults to TRUE
@Inherit	No	(0), defaults to FALSE
@AlternativeFieldSource	No	(NULL), defaults to not specified
@AlternativeFieldSourceTransform	No	(NULL) , defaulting to not specified

Additional data capture

ControlPoint MetaStore includes the database schemas, **Metadata** and **ControlPointMetadata**.

Metadata and the corresponding tables (for example, **Metadata.Document**) are used for the default set of captured properties only. Extensions to this default set must be captured into the **ControlPointMetadata** schema instead.

- If the additional data to be captured is a single value field (SVF), then it must be captured in the **ControlPointMetadata.Additional** table.
- If the additional data to be captured is a multivalue field (MVF) instead, then a new table must be created within the **ControlPointMetadata** schema to accommodate the multiple values for each document.

All multivalue tables should also include a repository identifier and a MD5 hash of the document DREREFERENCE. **ControlPointMetadata** also comprise of hash table types. These tables are utilized to reduce the storage footprint for information that is readily repeated. Each hash table has the same basic format comprising a repository identifier, a raw value and a MD5 hash of the raw value.

Examples

This section documents the steps required to capture additional metadata into ControlPoint MetaStore. It uses a number of examples to do so and includes corresponding SQL statements that need to be loaded and executed.

The examples make use of metadata fields AU_DOCUMENT_EDITOR_STRING and AU_DOCUMENT_AUTHOR_STRING to illustrate the differences between SVF and MVF table setup.

For any new field that is added to metadata, it needs to be added to the appropriate field type in FieldTypeInfo.

NOTE: AU_DOCUMENT_AUTHOR_STRING is already captured in ControlPoint MetaStore by default.

Example 1: Single value for the same document

Documents comprise a single `AU_DOCUMENT_EDITOR_STRING` value.

This will be recorded in the **ControlPointMetadata.Additional** table in a new field named **LastEditedBy**. Data mappings must be configured to instruct the MetaStore service on how to capture and record this field value during document ingestion.

To map data

1. In SQL Server, add a new column to the **ControlPointMetadata.Additional** table to support the capture of the `AU_DOCUMENT_EDITOR_STRING` string value:

```
USE ControlPointMetaStore
GO
ALTER TABLE ControlPointMetadata.Additional
ADD LastEditedBy NVARCHAR(255) NULL
GO
```

2. Configure `AU_DOCUMENT_EDITOR_STRING` data mapping using the `MetaStore.MapField` stored procedure:

```
USE ControlPointMetaStore
GO
EXEC MetaStore.MapField
@SourceName          = 'AU_DOCUMENT_EDITOR_STRING',
@TargetTable         = 'ControlPointMetadata.Additional',
@TargetColumn        = 'LastEditedBy',
@TargetTransform     = 'ToString'
GO
```

3. Refresh document ingest, import and update sequences to support the newly captured `AU_DOCUMENT_EDITOR_STRING` field in MetaStore.

```
USE ControlPointMetaStore
GO
EXEC MetaStore.ConfigureAddDocument
EXEC MetaStore.ConfigureUpdateDocument
EXEC ControlPointMetadata.ConfigureImportDocument
GO
```

4. Restart the ControlPoint MetaStore service to utilize the refreshed sequences.
5. If you add custom fields in Insert Configuration, you must restart the ControlPoint Engine.

Example 2: Single value hash for the same document

Documents comprise a single `AU_DOCUMENT_EDITOR_STRING` value. This example assumes that this string value is readily repeated throughout.

A new hash table, **ControlPointMetadata.EditorHash**, will be created to help reduce storage footprint.

A MD5 hash of AU_DOCUMENT_EDITOR_STRING will be recorded in the **ControlPointMetadata.Additional** table in a new field named **LastEditedByHash**. Data mappings must be configured to instruct the MetaStore service on how to capture and record this field value during document ingestion

To map data

1. Create a new hash table, **ControlPointMetadata.EditorHash**, to support the AU_DOCUMENT_EDITOR_STRING string value and MD5 hash value mappings.

```
USE ControlPointMetaStore
GO
IF OBJECT_ID(N'ControlPointMetadata.EditorHash', N'U') IS NULL
BEGIN
CREATE TABLE ControlPointMetadata.EditorHash
(
    RepositoryId    INTEGER          NOT NULL,
    HashKey         BINARY(8)        NOT NULL,
    Value           NVARCHAR(255)    NOT NULL,
    CONSTRAINT ControlPointMetadata_EditorHash_PK
    PRIMARY KEY NONCLUSTERED(RepositoryId, HashKey) WITH FILLFACTOR = 80
)
END
GO
```

2. Add a new column to the **ControlPointMetadata.Additional** table to support the MD5 hash of the AU_DOCUMENT_EDITOR_STRING string value.

```
USE ControlPointMetaStore
GO
ALTER TABLE ControlPointMetadata.Additional
ADD LastEditedByHash BINARY(8) NULL
GO
```

3. Create a foreign key relationship from the source table to the corresponding hash table.

```
USE ControlPointMetaStore
GO
ALTER TABLE ControlPointMetadata.Additional
ADD CONSTRAINT ControlPointMetadata_Additional_FK_LastEditedByHash
FOREIGN KEY (RepositoryId, LastEditedByHash)
REFERENCES ControlPointMetadata.EditorHash(RepositoryId, HashKey)
GO
```

4. Configure AU_DOCUMENT_EDITOR_STRING data mapping using the MetaStore.MapField stored procedure.

```
USE ControlPointMetaStore
GO
EXEC MetaStore.MapField
@SourceName        = 'AU_DOCUMENT_EDITOR_STRING',
@TargetTable       = 'ControlPointMetadata.Additional',
@TargetType        = 'SVF',
@TargetColumn      = 'LastEditedByHash',
@TargetTransform   = 'HashValue',
```

```
@SupportingTable      = 'ControlPointMetadata.EditorHash'  
GO
```

5. Refresh document ingest, import and update sequences to support the newly captured AU_DOCUMENT_EDITOR_STRING field in ControlPoint MetaStore.

```
USE ControlPointMetaStore  
GO  
EXEC MetaStore.ConfigureAddDocument  
EXEC MetaStore.ConfigureUpdateDocument  
EXEC ControlPointMetadata.ConfigureImportDocument  
GO
```

6. Restart the ControlPoint MetaStore service to utilize the refreshed sequences.
7. If you add custom fields in Insert Configuration, you must restart the ControlPoint Engine.

Example 3: Multiple values for the same document

Documents can comprise multiple AU_DOCUMENT_AUTHOR_STRING values. These will be recorded in the **ControlPointMetadata.Author** table. Data mappings must be configured to instruct the MetaStore service on how to capture and record these field values during document ingestion.

To map data

1. Create a table, **ControlPointMetadata.Author** to record all AU_DOCUMENT_AUTHOR_STRING values for each document.

```
USE ControlPointMetaStore  
GO  
IF OBJECT_ID(N'ControlPointMetadata.Author', N'U') IS NULL  
BEGIN  
CREATE TABLE ControlPointMetadata.Author  
(  
    RepositoryId          INTEGER          NOT NULL,  
    DocKey                BINARY(8)        NOT NULL,  
    Author                NVARCHAR(255)    NOT NULL  
CONSTRAINT ControlPointMetadata_Author_PK  
PRIMARY KEY CLUSTERED(RepositoryId, DocKey, Author)  
WITH FILLFACTOR = 80  
)  
END  
GO
```

2. Configure AU_DOCUMENT_AUTHOR_STRING data mapping using the MetaStore.MapField stored procedure.

```
USE ControlPointMetaStore  
GO  
EXEC MetaStore.MapField  
    @SourceName          = 'AU_DOCUMENT_AUTHOR_STRING',  
    @TargetTable         = 'ControlPointMetadata.Author',  
    @TargetType          = 'MVF',
```

```
@TargetColumn          = 'Author',  
@TargetTransform       = 'ToString'  
GO
```

3. Refresh document ingest, import and update sequences to support the newly captured AU_DOCUMENT_AUTHOR_STRING field in MetaStore.

```
USE ControlPointMetaStore  
GO  
EXEC MetaStore.ConfigureAddDocument  
EXEC MetaStore.ConfigureUpdateDocument  
EXEC ControlPointMetadata.ConfigureImportDocument  
GO
```

4. Restart the ControlPoint MetaStore service to utilize the refreshed sequences.
5. If you add custom fields in Insert Configuration, you must restart the ControlPoint Engine.

Example 4: Multiple values hashed for the same document

Documents can comprise multiple AU_DOCUMENT_AUTHOR_STRING values. This example assumes that these string values are readily repeated throughout.

A new hash table, **ControlPointMetadata.AuthorHash**, will be created to help reduce storage footprint. Hashed AU_DOCUMENT_AUTHOR_STRING values for each document will be stored in **ControlPointMetadata.Author**. Data mappings need configured to instruct the MetaStore service on how to capture and record these field values during document ingestion.

To map data

1. Create a new hash table, **ControlPointMetadata.AuthorHash**, to support the AU_DOCUMENT_AUTHOR_STRING string value and MD5 hash value mappings.

```
USE ControlPointMetaStore  
GO  
IF OBJECT_ID(N'ControlPointMetadata.AuthorHash', N'U') IS NULL  
BEGIN  
CREATE TABLE ControlPointMetadata.AuthorHash  
(  
    RepositoryId    INTEGER          NOT NULL,  
    HashKey         BINARY(8)        NOT NULL,  
    Value           NVARCHAR(255)    NOT NULL,  
    CONSTRAINT ControlPointMetadata_AuthorHash_PK  
    PRIMARY KEY NONCLUSTERED(RepositoryId, HashKey) WITH FILLFACTOR = 80  
)  
END  
GO
```

2. Create a table, **ControlPointMetadata.Author** to record all MD5 hashes for AU_DOCUMENT_AUTHOR_STRING values for each document.

```
USE ControlPointMetaStore  
GO
```

```
IF OBJECT_ID(N'ControlPointMetadata.Author', N'U') IS NULL
BEGIN
CREATE TABLE ControlPointMetadata.Author
(
    RepositoryId    INTEGER          NOT NULL,
    DocKey          BINARY(8)       NOT NULL,
    AuthorHash     BINARY(8)       NOT NULL
CONSTRAINT ControlPointMetadata_Author_PK
PRIMARY KEY CLUSTERED(RepositoryId, DocKey, AuthorHash)
WITH FILLFACTOR = 80,
CONSTRAINT ControlPointMetadata_Author_FK_AuthorHash
FOREIGN KEY (RepositoryId, AuthorHash)
REFERENCES ControlPointMetadata.AuthorHash(RepositoryId, HashKey)
)
END
GO
```

3. Configure AU_DOCUMENT_AUTHOR_STRING data mapping using the MetaStore.MapField stored procedure.

```
USE ControlPointMetaStore
GO
EXEC MetaStore.MapField
    @SourceName      = 'AU_DOCUMENT_AUTHOR_STRING',
    @TargetTable     = 'ControlPointMetadata.Author',
    @TargetType      = 'MVF',
    @TargetColumn    = 'AuthorHash',
    @TargetTransform = 'HashValue',
    @SupportingTable = 'ControlPointMetadata.AuthorHash'
GO
```

4. Refresh document ingest, import and update sequences to support the newly captured AU_DOCUMENT_AUTHOR_STRING field in MetaStore.
5. Restart the ControlPoint MetaStore service to utilize the refreshed sequences.
6. If you add custom fields in Insert Configuration, you must restart the ControlPoint Engine.

Existing data and re-ingestion

The steps outlined in the examples ensure that the new field, AU_DOCUMENT_EDITOR_STRING, is captured for new document files being ingested.

Existing data will need to be re-ingested in order to capture values for this new metadata field.

NOTE: If you add custom fields in Insert Configuration, you must restart the ControlPoint Engine so that ControlPoint picks up the new custom fields.

To re-ingest data

- Select **Re-Index Repository** on the Repositories dashboard.
- Remove the connector database file from the connector installation directory, followed by a connector service restart.

Field text and advanced properties

The new metadata has been captured into ControlPoint MetaStore through document ingestion. In order to make use of this new data for field text purposes and to return as part of the Properties/Advanced Properties within the ControlPoint Dashboard, a number of further changes are required.

Field text

In order to make the new field available within the category field text builder, a new Rule Builder Fields mapping must be configured within the ControlPoint Administration Dashboard.

To support this, a database view modification must be made to ensure the new field is available from the list of rule builder available fields in the ControlPoint UI.

To add a new field within the category field text builder

1. Open SQL Management Studio and expand **Databases > ControlPointMetaStore > Views**.
 - a. Select **MetaStorePro.FieldTypeInfo**, right click and click **Script View as > Alter To > New Query Editor Window**.

NOTE: For any new field that is added, it needs to be added to the appropriate field type in `FieldTypeInfo`.

Examples:

- A new field, `AU_DOCUMENT_EDITOR_STRING`, must be appended to both 'Match' and 'RulesBuilderInc' `FieldType` list of supported fields and then executed.
 - A new date field must be appended to both the 'NumericDate' and 'RulesBuilderInc' `FieldType` list of supported fields and then executed.
2. On the ControlPoint Administration dashboard, click **Settings**.

The Settings page opens.

 - a. On the General tab, select **Fields**. In the Rule Builder section, add a new field by clicking **Add (+)**.

The Add New Field page opens.
 - b. Enter a name for the new field in the **Display Name** box.

- c. Select the new metadata field from the **Fields** list.
- d. Click **Add**.

After the new field mapping is added, the new metadata captured into MetaStore can be used for category training purposes.

Properties and advanced properties

The new field is available within the ControlPoint UI in the Advanced Properties list after you restart Internet Information Service (IIS).

To configure a new property mapping

1. On the ControlPoint Administration dashboard, click **Settings**.
The Settings page opens.
2. On the General tab, select **Fields**. In the Item Properties section, add a new item property by clicking **Add (+)**.
The Add Property page opens.
3. Enter a name for the new property in the **Display Name** box.
4. Select the type from the **Type** list.
5. Select the new metadata field from the **Fields** list.
6. Click **Add**.

Chapter 17: ControlPoint multi-domain configuration

This chapter describes the procedure to set up and use the multi-domain feature.

To configure the ControlPoint domain feature

1. Prepare your environment with all required [prerequisites](#).
2. [Configure multi-domain support](#).
3. [Test your multi-domain configuration](#)

Prerequisites

The following list identifies the prerequisites for setting up the multi-domain feature.

1. Deploy ControlPoint on machines under primary domain only.
2. For any machine under non-primary domain, deploy only the Connector and Connector framework.
3. Ensure that a two-way trust relationship exists between the primary domain and all non-primary domains. You must also ensure that all the primary domain users that use ControlPoint, can query all non-primary domains LDAP/AD.
4. For all non-primary domains, create a domain user to install and run Connector and Connector framework. This user should be able to query LDAP/AD to get all domain user information.
5. Ensure all machines with ControlPoint or IDOL components installed can communicate with each other.
6. In order to move files successfully across different domains, ensure the temp location is accessible by all domain users that runs Connector.
7. Ensure the domain name and domain root **DN** are ready to use. For example, for domain `cp.test.com`, the domain name is `cp` and the domain root DN is `DC=cp,DC=test,DC=com`.
8. To scan the source files, it is strongly recommended to use Connector under same domain.

Configure multi-domain support

To configure multi-domain support

1. In the ControlPoint user interface, click **Administration** -> **Additional Domain Registration**, and then set the non-primary domain for ControlPoint with domain name and domain root DN.
2. Install the Connector and Connector frameworks on machines under non-primary domain. Ensure that you copy the **commons** folder to the installed machine and update the following parameters with correct information in Connector configuration file. You must also ensure that this machine can communicate with all other machines that appear in the configuration.

```
[License]
LicenseServerHost=HOSTNAME //in Primary Domain
.....

[DistributedConnector]
Host=HOSTNAME //in Primary Domain
Port=PORT_NUMBER
ConnectorGroup=Filesystem_DOMAINNAME
.....

[Ingestion]
IngestHost=CFS_HOSTNAME //in Secondary Domain
IngestPort=PORT_NUMBER
.....

[Connector]
FieldNameDictionaryPath=COMMONS_FOLDER_PATH\fieldNormalizationData/connectors_
dictionary.xml
.....

[ImportService]
KeyviewDirectory=COMMONS_FOLDER_PATH\filters
.....

[FetchTasks]
PathRegex=.*
ForceDelete=true
MappedSecurity=True
```

```
GroupServerHost=OGS_HOSTNAME //in Primary Domain
GroupServerPort=OGS_PORT
GroupServerRepository=LDAP
.....
[ViewServer]
EnableViewServer=TRUE
Host=VIEWER_HOSTNAME //in Secondary Domain
Port=PORT_NUMBER
```

3. Update the following parameters in the CFS configuration files.

```
[License]
LicenseServerHost=HOSTNAME //in Primary Domain
.....
[ImportService]
KeyviewDirectory=COMMONS_FOLDER_PATH\filters
FieldNameDictionaryPath=COMMONS_FOLDER_PATH\fieldNormalizationData/connectors_
dictionary.xml
.....
[MyIdolIndexer]
DREHost=HOSTNAME //in Primary Domain
ACIPort=PORT
[MyMetastoreIndexer]
Type=Metastore
Host=HOSTNAME //in Primary Domain
Port=PORT
[Classifier]
DREHost=HOSTNAME //in Primary Domain
ACIPort=PORT
```

4. Set OGS to support multiple domains. The file contains more than one LDAP section so you must use [LDAP] for the name of the combined repository. It returns combined results from each [LDAPX] section.

Also, the order set for the `GroupServerDefaultRepositories` is very important. Ensure that you add the individual repositories before the combined one. For example:

```
GroupServerDefaultRepositories=LDAP1,LDAP2
```

```
Number=3
0=LDAP1
1=LDAP2
2=LDAP
[LDAP]
GroupServerJobType=LDAP
GroupServerSections=LDAP1,LDAP2
GroupServerStartDelaySecs=10
GroupServerCycles=-1
[LDAP1]
GroupServerLibrary=ogs_ldap.dll
LDAPServer=LDAP_SERVER_HOST
LDAPPort=PORT
LDAPBase=LDAP_BASE
LDAPType=MAD
LDAPUsername=LDAP_DISTINGUISHED_NAME (e.g., LDAPUsername=CN=CPADMIN
CPADMIN,DC=qa,DC=englab,DC=local)
LDAPPassword=PASSWORD
LDAPBindMethod=NEGOTIATE
GroupServerAllUserGroups=NT AUTHORITY\AUTHENTICATED USERS
GroupServerCycles=-1
UseDomainPrefix=True
DomainPrefix=DOMAIN_NAME //e.g., Primary Domain
[LDAP2]
GroupServerLibrary=ogs_ldap.dll
LDAPServer=LDAP_SERVER_HOST
LDAPPort=PORT
LDAPBase=LDAP_BASE
LDAPType=MAD
LDAPUsername=LDAP_DISTINGUISHED_NAME
LDAPPassword=PASSWORD
LDAPBindMethod=NEGOTIATE
```

```
GroupServerAllUserGroups=NT AUTHORITY\AUTHENTICATED USERS
```

```
GroupServerCycles=-1
```

```
UseDomainPrefix=True
```

```
DomainPrefix=DOMAIN_NAME //e.g., Secondary Domain
```

5. Restart the OGS service and ensure the OGS can create a database for each [LDAPX]
6. Create a non-primary domain through the ControlPoint admin interface. There is cache for domain information, which gets updated periodically. You can change the timeout value in the ControlPoint database. If you want the change to be taken effect immediately instead of waiting for cache timeout, restart IIS.

Test your multi-domain configuration

After set up, Micro Focus strongly recommends you test your multi-domain configuration.

To test your multi-domain configuration

1. Ensure the Connector and CFS deployed on the non-primary domain are running and work without any problems.
2. Ensure all Connectors are registered. To verify, distribute Connector with query `http://hostname:7000/Action=getstatus`.
3. Ensure OGS captures the correct information. To do so, use the query `http://hostname:4057/Action=GetGroups&UserName=DOMAINUSERNAME&Repository=LDAP`
4. In ControlPoint, create a domain user in the non-primary domain and log in as that user to ensure login works correctly.
5. Create a repository in the non-primary domain with the correct Connector. If you get an error message that states "shared location may not be reached", ignore it and click **Save**.
6. Verify the Connector and ensure ingestion works.
7. Open the browser repository and ensure that the system administrator can view all documents.
8. Open the browser repository as user (not a superuser) and ensure the user can access only their documents.

Appendix A: ControlPoint Support utility

The ControlPoint Support utility captures system information and configuration file information from your ControlPoint environment.

The utility supports the following modes:

- **User interface.** Captures the information and generates a ZIP archive of the results and the report file.
- **Command line.** For command line options and examples, see [Synopsis, below](#).

Location

```
\Program Files\Micro  
Focus\ControlPoint\Engine\Scheduler\ControlPointSupportUtility.exe
```

Synopsis

```
ControlPointSupportUtility.exe  
ControlPointSupportUtility.exe -c
```

Options

- **No option.** Generates a ZIP archive of the results and the xml/xslt browser report file.
- **-c.** Moves the data to the <systemroot>\<user>\AppData\Local\Temp directory for comparison. Does not generate a ZIP archive of the results or the report file.

To generate a report that contains comparison results, you must run the utility with the -c option twice.

Example

Run the utility as a preparatory step when changing the ControlPoint environment.

1. Run the Support utility from the command line as the Administrator.

```
ControlPointSupportUtility.exe -c
```

The utility gathers a copy of all system and configuration file information and stores it labeled as Pre capture data.

2. Perform the changes to the environment.
3. Run the Support utility to gather the data and label it as Post data.

```
ControlPointSupportUtility.exe -c
```

The utility runs a comparison feature, which generates a report named `diffReport.txt`. The ControlPoint Support utility creates the report in the same directory as the utility.

The report lists any differences between the two `SystemInfo.xml` files, including changes, additions, and deletions. In addition, it lists any differences between all configuration files located in the ControlPoint installation directory.

Results

When the utility is run with the `-c` option, it stores the Pre and Post data files in `<systemroot>\Users\<user>\AppData\Local\Temp`.

Appendix B: Configure ControlPoint security settings

If you enabled ControlPoint security while installing ControlPoint or had it previously enabled and then upgraded ControlPoint, you must finish configuring security by updating settings in several configuration files.

NOTE: After updating all files, restart the ControlPoint services for each component whose file you updated. For information how to do this, see [Start Windows services, on page 35](#).

Update the following ControlPoint configuration files with the settings **in bold**:

- [ControlPoint IDOL configuration](#)
- [ControlPoint OGS configuration](#)
- [Documentum Connector configuration](#)
- [Filesystem Connector configuration](#)
- [SharePoint Remote Connector configuration](#)

ControlPoint IDOL configuration

File: Program Files\Micro Focus\ControlPoint\Indexer\IDOL\ControlPoint IDOL.cfg

```
9=NT
[NT]
GroupServerHost=OGSHostName
GroupServerPort=OGSPort
GroupServerRepository=LDAP

[LDAP]
LDAPServer=LDAPServerHostName
LDAPPort=389

[SharePoint]
GroupServerHost=OGSHostName
GroupServerPort=OGSPort
GroupServerRepository=Combine

[Documentum]
DocumentSecurity=TRUE
GroupServerHost=OGSHostName
GroupServerPort=OGSPort
SecurityFieldCSVs=username
DocumentSecurityType=Documentum_V4
```

```
CaseSensitiveUserNames=FALSE
CaseSensitiveGroupNames=FALSE
GroupServerPrefixDomain=FALSE
GroupServerOpApplyTo=USER
GroupServerOp=Prepend
GroupServerOpParam=YourDomainName\      (Example: GroupServerOpParam=myCompany\)
```

ControlPoint OGS configuration

File: Program Files\Micro Focus\ControlPoint\Indexer\OGS\ControlPoint OGS.cfg

[License]

```
LicenseServerHost=LicenseServerHostName
LicenseServerACIPort=20000
LicenseServerTimeout=600000
LicenseServerRetries=1
```

[Repositories]

```
GroupServerDefaultRepositories=HPRecordsManager,TRIM,SharePoint2007,SharePoint2010,
SharepointRemote,WorkSite,SharePoint2013,Documentum,LDAP,Combine
```

Number=10

```
0=HPRecordsManager
1=TRIM
2=Sharepoint2007
3=Sharepoint2010
4=SharepointRemote
5=WorkSite
6=Sharepoint2013
7=Documentum
8=LDAP
9=Combine
```

[LDAP]

```
GroupServerLibrary=ogs_ldap.dll
LDAPServer=LDAPServerHostName
LDAPPort=389
LDAPBase=DC=BaseDN      (Example: LDAPBase=DC=myCompany,DC=com)
LDAPType=MAD
LDAPBindMethod=NEGOTIATE
GroupServerAllUserGroups=NT AUTHORITY\AUTHENTICATED USERS
GroupServerCycles=-1
UseDomainPrefix=TRUE
DomainPrefix=DomainPrefix      (Example: DomainPrefix=myCompany)
```

[Combine]

```
GroupServerJobType=Combine
GroupServerSections=LDAP,SharepointRemote
```

```
GroupServerStartDelaySecs=10  
GroupServerCycles=-1
```

[Documentum]

```
GroupServerLibrary=ogs_java  
JavaGroupServerClass=com.autonomy.groupserver.documentum.DocumentumGroupServer  
Docbase=CustomDocBase (Case-sensitive)  
Username=UserName (Case-sensitive)  
Password=***** (Unencrypted plain text)  
GroupServerCycles=-1  
GroupServerQueryOp0=StartAfter  
GroupServerQueryOpApplyTo0=USER  
GroupServerQueryOpParam0=0;\  
GroupServerShowAlternativeNames=TRUE  
UserNameFields=user_login_name
```

[SharepointRemote]

```
GroupServerLibrary=ogs_text.dll  
GroupServerIncremental=TRUE  
Textfile=SharepointRemoteGS.txt  
ConnectorHost=ConnectorHostName  
ConnectorPort=ConnectorPort
```

Documentum Connector configuration

File: Program Files\Micro Focus\ControlPoint\Indexer\DocumentumConnector\ControlPoint
Documentum Connector.cfg

[Ingestion]

```
IngestActions=META:ENFORCESECURITY=True,META:CPREPOSITORYTYPEID=17,META:SECURITYTYPE  
=Documentum
```

[FetchTasks]

```
GroupServerHost=  
GroupServerPort=  
GroupServerRepository=  
HoldUseRetentionPolicy=  
HoldUseFreeze=  
HoldAllVersions=  
HoldUpdateAcl=  
mappedsecurity=
```

Filesystem Connector configuration

File: Program Files\Micro Focus\ControlPoint\Indexer\FileSystem Connector\ControlPoint
FileSystem Connector.cfg

[Ingestion]

IngestActions=META:ENFORCESECURITY=True,META:CPREPOSITORYTYPEID=3,META:SECURITYTYPE=
NT

[FetchTasks]

MappedSecurity=TRUE

GroupServerHost=*OGSHostName*

GroupServerPort=*OGSPort*

GroupServerRepository=LDAP

SharePoint Remote Connector configuration

NOTE: ControlPoint security supports SharePoint *Remote* repositories, only. Any security-related settings you configure for a SharePoint Remote connector associated with a SharePoint *Online* repository are ignored.

File: Program Files\Micro Focus\ControlPoint\Indexer\SharePoint Remote
Connector\ControlPoint SharePoint Remote Connector.cfg

[Ingestion]

IngestActions=META:ENFORCESECURITY=True,META:CPREPOSITORYTYPEID=9,META:SECURITYTYPE=
SharePointSecurity

[FetchTasks]

GroupServerHost=*OGSHostName*

GroupServerPort=*OGSPort*

GroupServerRepository=SharepointRemote

EncryptACLEntries=FALSE

MappedSecurity=TRUE

Appendix C: Configure ControlPoint with IDOL Media Server

ControlPoint features include the ability to extract text from electronic formats such as documents, emails, and spreadsheets, as well as many other formats. You can perform sensitive data analysis on the extracted text using Education grammars and use Auto-Categorization of file content to organize the repository for policy execution. If the source repository contains scanned images, you can extract text from them by configuring the IDOL Media Server with the supported ControlPoint connectors. The extraction process uses Optical Character Recognition (OCR) from the scanned documents for Education and Categorization.

The default ControlPoint license package does not include an IDOL Media Software license. You must download, install, and obtain a license for IDOL Media Server in addition to ControlPoint. This appendix provides the steps to configure the IDOL Media Server to enable OCR of source repositories within ControlPoint.

Detailed IDOL Media Server documentation is available from the [Micro Focus IDOL documentation site](#).

Before you begin

Ensure you have the following items:

- Micro Focus IDOL Media Server software
The Media Server software is available as part of IDOL. If you have the appropriate software entitlements, you can download it from the [Licensing and Downloads page](#) of the Micro Focus Support site.
- An IDOL license with media server enabled

If you need help obtaining either of these items, contact your ControlPoint support representative.

To configure ControlPoint with IDOL Media Server

1. Extract the IDOL Media Server from its package, and then install it.

For example, install it to Program Files\Micro Focus\MediaServer.

TIP: The Media Server can use a lot of resources so Micro Focus recommends that you install it on a dedicated server.

2. (Optional) Configure the Media Server as a service so it automatically starts at system boot.

For example, the following configures it as a new service named "CPMediaServer":

```
CPMediaServer -Name "ControlPoint MediaServer" -BinaryPathName "C:\Program Files\Micro Focus\MediaServer\mediaserver.exe" -StartupType Automatic -Description "MediaServer for ControlPoint"
```

3. Configure the `mediaServerInstallPath\MediaServer.cfg` file:
 - a. Open the `MediaServer.cfg` file in a text editor.
 - b. Locate the `[Channels]` section and ensure `VisualChannels` is set to 1.
 - c. Locate the `[Server]` section and make note of the specified port number.

The default port is 14000, which you can change if necessary. You will use this value in a subsequent step.
 - d. If you have updated any values, save the file.
4. Configure the `ControlPoint\Indexer\FileSystem Connector Framework\ControlPoint Filesystem Connector framework.cfg` file:
 - a. Open the file in a text editor.
 - b. In the `[ImportTasks]` section, locate the `PreXX` lines, and then add the following `Pre2` line, incrementing any existing `Pre2` line to `Pre3`, and so on:

```
Pre2=lua:scripts/mediaserver/OCR.lua
```
 - c. Add a `[MediaServerSettings]` section after the `[ImportTasks]` section:

```
[MediaServerSettings]
MediaServerHost=localhost
MediaServerPort:port
ReadFromOriginalLocation=true
```

Where:

 - **localhost** is the name of the server where you installed `MediaServer` if its different than the one that hosts the `FileSystem Connector Framework`. Otherwise, set it to `localhost`.
 - **port** is the port number specified in the `[Server]` section of the `MediaServer.cfg` file that you noted in Step 3.
 - d. Save the file.
5. Update the `ControlPoint\Indexer\Filesystem Connector Framework\scripts\MediaServer\OCR.lua`:
 - a. Open the `OCR.lua` file in a text editor.
 - b. Move line 63 ("end") to line 67 (after the `document:addField` line), as follows in this snippet of the file:

```
});

end Move this line...
-- If analysis was performed successfully, don't extract
-- text using KeyView, just get the metadata.

document:addField("AUTN_FILTER_META_ONLY", "");

end ...to here
```

```
        return true;  
    end
```

c. Save the file.

6. Restart the **ControlPoint FileSystem Connector Framework** service using Windows Services.
7. Start either the *mediaServerInstallPath*\MediaServer\mediaserver.exe or the MediaServer service, and then wait a few minutes for it to become ready for use.

To verify that the Media Server started successfully, check its log files (*mediaServerInstallPath*\MediaServer\logs*.log).

Send documentation feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Micro Focus ControlPoint 5.9.0 Installation Guide

Add your feedback to the email and click **Send**.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to swpdl.controlpoint.docfeedback@microfocus.com.

We appreciate your feedback!