ControlPoint

Software Version 5.6.1

Installation Guide

Document Release Date: December 2018
Software Release Date: December 2018

Legal notices

Copyright notice

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are 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.

You can check for more recent versions of a document through the MySupport portal. Many areas of the portal, including the one for documentation, require you to sign in with a Software Passport. If you need a Passport, you can create one when prompted to sign in.

Additionally, if you subscribe to the appropriate product support service, you will receive new or updated editions of documentation. Contact your Micro Focus sales representative for details.

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:

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

Many areas of the portal require you to sign in with a Software Passport. If you need a Passport, you can create one when prompted to sign in. To learn about the different access levels the portal uses, see the Access Levels descriptions.

Contents

Chapter 1: Introduction 9

ControlPoint product suite 9

The Micro Focus IDOL platform 9

ControlPoint architecture 10

Components 10

ControlPoint Dashboard 10

ControlPoint Engine 10

ControlPoint Data Analysis service 10

ControlPoint IDOL 11

Related documentation 11

Chapter 2: Plan for a ControlPoint installation 13

Installation tasks 13

Prerequisites 13

ControlPoint requirements 14

Minimum hardware requirements - ControlPoint database server 14

Minimum hardware requirements - other ControlPoint servers 14

Software Requirements 15

Performance considerations 18

Antivirus recommendations 18

5.6.0.140\ControlPoint\5.6.0\ControlPoint Database Installer.exeCompatibility matrix 18

Supported browsers 19

Topology example 19

SQL Server deployment considerations 19

Example 19

Chapter 3: Install the ControlPoint databases 21

Database overview 21

Benefits 21

Recovery model for ControlPoint databases 22

Install and configure SQL Server 22

Configure the ControlPoint data source 22

Before you begin 23

Review the prerequisites 23

Minimum SQL permissions 24

Start the SQL Server Agent service 24

Read and write permissions on paths 24

Local volumes for database files 24

Logical file groups and the ControlPoint database installation program 24

Example 25

Install the ControlPoint databases 25

Next steps 30

Verify the new SQL maintenance jobs 30

Move ControlPoint databases 31

Chapter 4: Install ControlPoint IDOL and connectors 33

Overview 33

Create deployment packages 33

Configure deployment packages 33

Save deployment package configuration 37

Build deployment packages 37

Install deployment packages 37

Prerequisites 38

IDOL license key 38

Installation 38

IDOL Content language type setup 39

Start Windows services 39

Stop Windows services 39

Deploy multiple MetaStore services 39

Before you begin 40

Deploy the additional MetaStore component 40

Modify the Install and Uninstall MetaStore scripts 41

Modify the Install Services script 41

Modify the Start Services script 41

Modify the Stop Services script 42

Associate Connector Framework Services (CFS) to the new MetaStore component 42

Uninstall deployment packages 42

Chapter 5: Install ControlPoint components 43

Federal Information Processing Standards (FIPS) security mode 43

Before you begin 43

Limitations 43

Install ControlPoint and the ControlPoint Engine 43

Configure ControlPoint 44

Before you begin 44

Create a decoupled IDOL database repository 47

Deploy ControlPoint by enabling HTTPS 50

Enable HTTPS 50

Create certificates 50

Configure certificates in IIS Manager 51

Update the configuration files 52

Redeploy ControlPoint when HTTPS is enabled 53

Enable ControlPoint workflow capability with ControlPoint HTTPS deployment (optional) 53

5.6.0.140\ControlPoint\5.6.0\ControlPoint Database Installer.exeConfigure the Redirector service for HTTPS 53

Limitations 54

Create certificates 54

Bind certificate with a port 54

Redirector service HTTPS configuration 54

Chapter 6: Install ControlPoint Edge Filesystem connector 56
- Prerequisites 56
- Install the Edge Filesystem connector 56
- Edge Filesystem Connector configuration file 58
- Uninstall the Edge Filesystem connector 58

Chapter 7: Optimize IDOL configuration 59

Chapter 8: HTTPS setup for IDOL 61
- Set up HTTPS for IDOL and connectors 61
  - Create SSL certificates 61
  - Update the IDOL configuration 61
  - Enable TLS 1.2 protocol 70
  - ControlPoint settings to enable IDOL in HTTPS mode 71
- Stop IDOL services running with HTTPS 73
- Run the ControlPoint Configuration Manager with HTTPS enabled 73
- Troubleshooting 74
  - Verify HTTPS setup for IDOL 74
  - Repository page does not list registered repositories after changing the IDOL setup on HTTPS 75
  - ControlPoint Configuration Manager can not establish trust relationship 75

Chapter 9: IDOLv distributed mirror / non-mirror setup 77
- Introduction 77
- Mirror mode setup 77
- Non-mirror simple combinator mode setup 78
- Add exception in Windows Firewall 82

Chapter 10: Upgrade ControlPoint 83
- Overview of the upgrade process 83
- Before you begin 83
  - Run the Support Utility 84
- Prepare the ControlPoint environment for upgrade 84
- Uninstall the ControlPoint software 85
- Upgrade to ControlPoint 5.6.1 86
  - Upgrade the ControlPoint databases to 5.4 87
    - Obtain the ControlPoint 5.4 software 87
    - Upgrade the ControlPoint databases to 5.4 88
  - Upgrade the ControlPoint databases to 5.6.1 88
    - Recovery model for ControlPoint databases 89
    - Before you begin 89
      - Minimum SQL permissions 89
      - Read and write permissions on paths 89
    - Upgrade the databases 90
    - Post upgrade step 94
      - Verify the new SQL maintenance jobs 95
      - Move ControlPoint databases 95
  - ControlPoint databases and performance considerations 96
  - Install the ControlPoint software 97

Verify the databases in IDOL 97
Upgrade IDOL data and software 98
Upgrade the IDOL software manually 99
Update configuration files 100
Update Connector configuration files 100
Update Insert Configuration files 103
Update Insert Configurations for Micro Focus Content Manager connectors 103
Integrate IDOL proxy updates 103
Update Content Manager Connector configuration files 104
Post-upgrade steps 107
Rescan repositories with custom properties after the upgrade 109
Upgrade the Edge Filesystem connector 110
Edge Filesystem Connector configuration file 110
Chapter 11: Troubleshooting 112
Databases 112
Compact stored procedure 112
The Compact stored procedure takes more than several days to complete 112
Connectors 114
KeyView import.log failure if File System connector framework account and share permissions are not sufficient 114
CPCategory field is missing from the Advanced Properties during rescan of Connectors configured in SSL environments 114
Temporary files accumulate in different locations when indexing repositories 116
ControlPoint MetaStore service shows sustained very high memory and CPU usage and the Connector Framework service shows very high CPU usage 117
Edge Filesystem Connectors 118
Linux Edge Filesystem Connector in a distributed connector system does not belong to the same domain as ControlPoint 118
Unable to remove the DeleteArchive Policy once it is applied 118
SharePoint Connectors 118
EncryptACLEntries=False does not work if it is in the [Connector] section. 118
Content Manager connector 119
Insert into Content Manager fails when document title exceeds 128 characters 119
Proxy server interactions 119
Proxy server blocks traffic of Data Analysis service 119
IDOL 120
Preview of items on remote connectors 120
HTTPS setup for IDOL 120
Verify HTTPS setup for IDOL 120
Repository page does not list registered repositories after changing the IDOL setup on HTTPS 121
ControlPoint Configuration Manager can not establish trust relationship 122
IDOL distributed mirror / non- mirror setup 122
DAH stops working after the Content Engine stops running 122
Policy execution 123
Documents remain at 'Executing' state 123

Policy execution phase fails to acquire locks on any items 123
Delay in showing failed items as 'Failed' in the policy details page 124
Communications errors attempting to execute an action 124
Diagnostics logs 125
Policy Execution Logs 125
Data Analysis logs 126
Data Analysis service logs 126
Data Analysis Controller logs 126
Statistics Export utility trace logs 127

Chapter 12: Configure ControlPoint MetaStore for metadata ingestion 128
Data Mapping 128
MetaStore.MapColumn 128
MetaStore.MapTable 129
MetaStore.MapField 130
Additional data capture 131
Examples 131
Example 1 – single value for the same document 131
Example 2 – single value hash for the same document 132
Example 3 – multiple values for the same document 134
Example 4 – multiple values hashed for the same document 135
Existing data and re-ingestion 136
Field text and advanced properties 136
Field Text 137
Properties and Advanced Properties 137

Chapter 13: ControlPoint Multi-domain configuration 139
Prerequisites 139
Configure 139
Test 143

Appendix A: ControlPoint post-installation tasks 144
ControlPointTimer.exe.Config 144
Dashboard.config 144
ControlPoint IDOL cfg 145
ControlPoint OGS cfg 146
Filesystem Connector cfg 147
SharePoint Remote Connector cfg 147
Documentum Connector cfg 147

Appendix B: ControlPoint post-upgrade tasks 149
ControlPointTimer.exe.Config 149
Dashboard cfg 149
ControlPoint IDOL cfg 150
ControlPoint OGS cfg 151
Content.cfg 152
FileSystem Connector cfg 152
Filesystem Connector Framework cfg 153
SharePoint Remote Connector cfg 153

SharePoint Remote Connector Framework cfg 154
Documentum Connector cfg 154
Documentum Connector Framework cfg 155
Exchange Connector Framework cfg 156
Content Manager Connector Framework cfg 156
Notes Connector Framework cfg 157
Appendix C: ControlPoint Support utility 158
Appendix D: Configure ControlPoint with IDOL Media Server 160
Send documentation feedback 165

Chapter 1: Introduction

This chapter provides an overview of Micro Focus ControlPoint.

- ControlPoint product suite
- The Micro Focus IDOL platform
- ControlPoint architecture
- Related documentation

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*.

ControlPoint architecture

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

Components

ControlPoint includes the following components.

- ControlPoint Dashboard
- ControlPoint Engine
- ControlPoint Data Analysis
- ControlPoint IDOL Connectors

ControlPoint Dashboard

The ControlPoint Dashboard interface allows users to view repositories, establish and review allocation of policies, administer Micro Focus IDOL categories, and monitor system activity and health, depending on their roles.

The following services are included in the ControlPoint.

- **ControlPoint Web Interface** is an IIS Web application that serves as the ControlPoint user interface
- **CPWS** (optional). Web services that provide access to ControlPoint resources for ControlPoint Workflow capability

ControlPoint Engine

The ControlPoint Engine provides the central capability to manage policy content within an organization.

The following services are included in the ControlPoint Engine.

- **ControlPoint Engine service** is a Windows service that executes all scheduled tasks
- **CallbackHandler** is an IIS Web application that receives notifications from Micro Focus IDOL connectors
- **ControlPointLicenseService** is a 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 the IDOL licensing.

ControlPoint Data Analysis service

ControlPoint Data Analysis allows your organization to analyze, understand, and deal with the unstructured data contained in legacy repositories.ControlPoint uses IDOL to analyze the documents in the repositories, analyze them, and presents 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 following connector types can be deployed from ControlPoint IDOL Deploy Tool:

- The **ControlPoint IDOL** service contains the central index.
- The **ControlPoint Content** services index all of the content and serves search requests.
- The **ControlPoint Content Manager connector** service scans and performs actions on items in Content Manager repositories. This connector type has a connector framework deployed alongside.

  > **NOTE:**
  > With the release of ControlPoint 5.4, the Content Manager connector replaces the Micro Focus Records Manager and TRIM connectors. The Content Manager connector is compatible with Content Manager, Records Manager and TRIM repositories.

- The **ControlPoint OGS** (**Omni Group Server**) service collects and aggregates user and group security information from a variety of repositories.
- The **ControlPoint Exchange Connector** service scans and performs actions on items in Exchange repositories. This connector type has a connector framework deployed alongside.
- The **ControlPoint FileSystem Connector** service scans and performs actions on items in file shares. This connector type has a connector framework deployed alongside.
- The **ControlPoint Hadoop Connector** service scans and performs actions on items in Hadoop repositories. This connector type has a connector framework deployed alongside.
- The **ControlPoint SharePoint Remote Connector** service scans and performs actions on items in SharePoint 2016 and SharePoint Remote sites. This connector type has a connector framework deployed alongside.
- The **ControlPoint DataAnalysis Store** service analyzes, understands, and deals with the unstructured data contained in legacy repositories
- The **ControlPoint Distributed Connector** service distributes connector calls to the appropriate connector
- The **ControlPoint IDOL License Server** service controls the licensing of all ControlPoint functionality

Related documentation

The following documents provide more detail on ControlPoint.

- *ControlPoint Installation Guide*
- *ControlPoint Best Practices Guide*
- *ControlPoint Administration Guide*

- *ControlPoint Remote Analysis Agent Technical Note*
- *ControlPoint Support Matrix*

The following documents provide more detail on IDOL connectors.

- *IDOL Distributed Connector Administration Guide*
- *IDOL Exchange Connector (CFS) Administration Guide*
- *IDOL File System Connector (CFS) Administration Guide*
- *IDOL Hadoop Connector (CFS) Administration Guide*
- *IDOL SharePoint Remote Connector (CFS) Administration Guide*

Chapter 2: Plan for a ControlPoint installation

This section describes the prerequisites for a ControlPoint installation and provides some deployment examples.

- Installation tasks
- Prerequisites
- Performance considerations
- Antivirus recommendations
- 5.6.0.140\ControlPoint\5.6.0\ControlPoint Database Installer.exeCompatibility matrix
- Supported browsers
- Topology example

Installation tasks

The high-level tasks to perform to install ControlPoint are as follows:

1. Install the prerequisite hardware and software for the ControlPoint environment. See Prerequisites, below.
2. Install the ControlPoint databases, including the MetaStore database. For more information, see Install the ControlPoint databases, on page 21.
3. Identify and install IDOL and the connectors.
   - Install the ControlPointIDOL connectors using the included Deploy Tool package. See Install ControlPoint IDOL and connectors, on page 33.
   - Install the the ControlPoint Edge Filesystem connector. See Install ControlPoint Edge Filesystem connector, on page 56.
4. Install ControlPoint and the ControlPoint Engine.

   For more information, see Install ControlPoint and the ControlPoint Engine, on page 43.
5. After the installation is complete, update the Connector and Connector framework configuration files. For more information, see ControlPoint Post-installation tasks.

Prerequisites

This section lists the prerequisites for installing the various ControlPoint components.

ControlPoint requirements

Minimum hardware requirements - ControlPoint database server

Component	Requirement
Processors	• 64-bit environment ◦ Server class processors with 16 cores, with speeds of 2.5 GHz or better (minimum)
Memory	• 64-bit environment ◦ 32-GB RAM as a minimum, especially for the server hosting the ControlPoint databases.
Storage	Your particular scale requirements depend on many factors including data sizes, usage patterns, infrastructure and so on. To achieve scale requirements for your ControlPointenvironment, contact your Micro Focus Professional Services representative. For more information on ControlPoint database storage capacity considerations, see Performance considerations, on page 18.
Dedicated hard drives for 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 during installation. Micro Focus recommends the use of the fastest, performance-quality drives with the best I/O bandwidths available. For more information, contact your Micro Focus Professional Services representative. The volumes you use for the ControlPoint database files must be local to the server where SQL Server is installed. This is a SQL Server requirement.

Minimum hardware requirements - other ControlPoint servers

Component	Requirement
Processors	• 64-bit environment ◦ Server class processors with 16 cores, with speeds of 2.5 GHz or more (minimum)
Memory	• 64-bit environment ◦ 32-GB RAM as a minimum, especially for the server hosting the ControlPoint databases.
Network interface card	1 Gbps

Software Requirements

Install ControlPoint software on servers that have the following software installed:

Application	Requirements
Operating system	• Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 **NOTE:** If you upgrade Windows Server, you must then reinstall ControlPoint so the application can verify that required components, such as IIS and the .NET Framework, are still available. If it determines any have changed or are missing, the installation process alerts you to reinstall them. For more information, see your Windows Server documentation.
Windows 2012	On Windows Server 2012, enable Windows Communication Foundation (WCF) Services HTTP Activation. For more information, see your Microsoft Windows Server 2012 documentation.
Internet Information Server (IIS)	• IIS 8.5 on Windows Server 2012 R2 • IIS 8.0 on Windows Server 2012 • IIS 7.5 on Windows Server 2008 R2 **NOTE:** On Microsoft Windows Server 2008 R2, add the Windows Authentication Role, which is not installed by default. For more information, see your Windows Server documentation.
IIS	In IIS, when configuring the Web Server (IIS) role for the ControlPoint Administration Console, activate the following features: • Common HTTP Features, including Static Content.
Microsoft .NET Framework	Versions 3.5, 4.5 and later.
Internet Explorer	Version 9 or later, installed on servers with ControlPoint Data Analysis and IIS.
SQL Server	SQL Server must be accessible from the ControlPoint server. • SQL Server 2016 Enterprise or Standard, service pack 1 and later • SQL Server 2014 Enterprise or Standard, service pack 2 and later. • SQL Server 2012 Enterprise or Standard, service pack 3 and later

Application	Requirements
	- Ensure that SQL Server Native Client is installed. **NOTE:** To gain the best performance, Micro Focus recommends that you do not install any other ControlPoint components on the SQL Server. If you are deploying the ControlPoint databases to a server hosting other ControlPoint components, such as connectors, configure SQL Server to limit the resources it consumes. **NOTE:** For large-scale deployments, use Enterprise Edition of SQL Server, as it enables you to split the tables on different files and optimizes the performance.
SQL Server service packs and updates	For each version and edition of SQL Server, you need to apply all currently-available and pushed updates (critical updates and publicly-pushed individual updates) from Windows Update.
SQL Permissions	The user account that deploys or upgrades the ControlPoint databases must have permissions equivalent to the **sysadmin** default SQL login role. This includes the permission to add, delete and modify jobs SQL Agent jobs, which requires access to the **msdb**. It also includes permission to examine database and filegroup structures, adding new ones as appropriate. After deployment, the permissions of the SQL login account may be then reduced. The minimum required permissions for each of the ControlPoint databases' user is **db_owner**.
SQL Server Agent service	The SQL Server Agent service must be set to start automatically, and the service must be running.
SQL Server Reporting Services	For Reporting Services, you can use the Standard or Enterprise edition of SQL Server. For more information, see Configure the ControlPoint data source, on page 22.
Read/write permissions on database file paths	The desired paths to place the database file groups must be granted read and write permission appropriately. For more information, see Read and write permissions on paths, on page 24

Software requirements - IDOL and ControlPoint connectors

Application	Requirements
ControlPoint IDOL packages	Install the ControlPoint IDOL packages on a server that has the following products installed: • Microsoft Visual C++ 2005 Redistributable Package • Microsoft Visual C++ 2010 Redistributable Package • Microsoft Visual C++ 2013 Redistributable Package
ControlPoint Content Manager Connector and Content Manager client software	Install the Content Manager client software on the server hosting the ControlPoint Content Manager Connector. For more information on installing the Content Manager client software, see the *Content Manager Installation and Setup Guide.*
ControlPoint Console server and Content Manager client software	Install the Content Manager client software on the server hosting the ControlPoint Administration Console.
Content Manager permissions	The following permissions are required to set up the Content Manager Connector: • The user running the Content Manager Connector account must be added as trusted account in Content Manager Enterprise Studio. It impersonates the TRIMServices account when retrieving items from the Content Manager dataset for indexing into ControlPoint IDOL. • The user running the Content Manager Connector account must be also present as a valid location in Content ManagerContent Manager. This is needed when you browse a repository of the Content Manager type, through the ControlPoint Console. • The user running the ControlPoint Web Application Pool must be added as a trusted account in Content Manager Enterprise Studio. The ControlPoint Web App pool user impersonates the user logged in ControlPoint to retrieve the list of Origins from the dataset. • The user logged into ControlPoint must be a valid user in Content Manager, and must have sufficient rights to view the origins.

Performance considerations

Ensure that your environment meets all hardware, software, and third-party component requirements as described in the *ControlPoint Installation Guide* or *Support Matrix*.

For more information on general performance guidelines in ControlPoint and in SQL Server, see the *ControlPoint Installation Guide* and the *ControlPoint Best Practices Guide*.

Your particular scale requirements depend on many factors including data sizes, usage patterns, infrastructure and so on. To achieve scale requirements for your ControlPoint environment, contact your Micro Focus Professional Services representative.

Antivirus recommendations

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

Some 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.

5.6.0.140\ControlPoint\5.6.0\ControlPoint Database Installer.exeCompatibility matrix

ControlPoint and IDOL mapping

Component	Version	Operating System
Distributed Connector	10.8.1	Windows, Linux, Solaris
Edge FileSystem Connector	11.2	Windows, RHEL, Suse
Exchange Connector	10.11	Windows
File System Connector	11.2	Windows[1]
Hadoop Connector	10.10	Windows, RHEL, Suse, Solaris
Content Manager Connector	11.2	Windows
IDOL Server	11.2	Windows, Linux, Solaris
MetaStore	11.2	Windows
Notes	10.1	Windows, Linux
Omni Group Server	10.8	Windows
Sharepoint Connector Remote[2]	11.1	Windows

[1] Support includes file shares on: CIFS and NFS on NetApp storage, and NTFS.

[2] Support includes SharePoint 2016.

Supported browsers

- Internet Explorer 9 or later
- Google Chrome 41 or later

Topology example

This section describes an example for a distributed ControlPoint topology.

> **NOTE:**
> This is intended as an example. Your ControlPoint environment may be different based on your size and scale requirements.
>
> For assistance in sizing your ControlPoint environment, contact Micro Focus Professional Services.

SQL Server deployment considerations

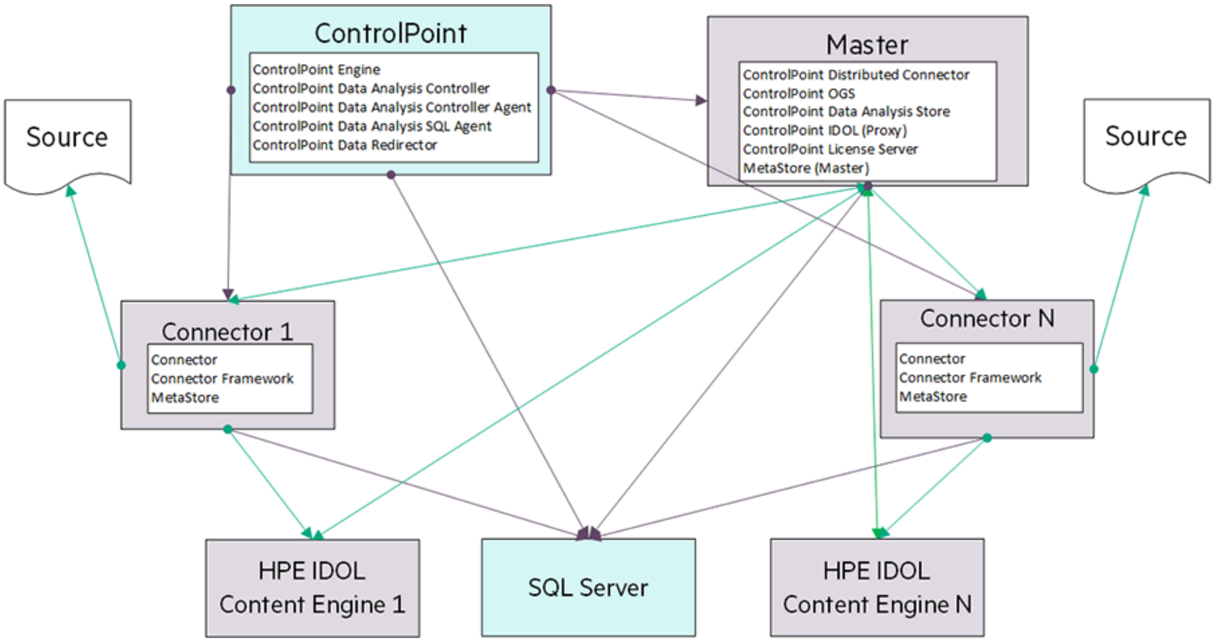
Micro Focus recommends that you deploy the SQL Server and the ControlPoint databases to a host containing no other ControlPoint components. This allows the configuration of SQL Server and the ControlPoint databases for the best performance.

If you deploy the ControlPoint databases to a server hosting other ControlPoint components, such as connectors, configure SQL Server to limit the resources it consumes.

The following examples assume that a separate SQL Server host is used to host the ControlPoint databases.

Example

ControlPoint system topology


ControlPoint
ControlPoint Engine
ControlPoint Data Analysis Controller
ControlPoint Data Analysis Controller Agent
ControlPoint Data Analysis SQL Agent
ControlPoint Data Redirector
Master
ControlPoint Distributed Connector
ControlPoint OGS
ControlPoint Data Analysis Store
ControlPoint IDOL (Proxy)
ControlPoint License Server
MetaStore (Master)
Source
Source
Connector 1
Connector
Connector Framework
MetaStore
Connector N
Connector
Connector Framework
MetaStore
HPE IDOL
Content Engine 1
SQL Server
HPE IDOL
Content Engine N

Chapter 3: Install the ControlPoint databases

The ControlPoint environment contains the following five databases.

- ControlPoint
- ControlPoint Audit
- ControlPointMetaStore
- ControlPointMetaStore Tags
- ControlPoint Tracking

Database overview

The ControlPoint 5.5 release allows for SQL Server storage separation to multiple storage paths per database. This allows you to use more of the discrete, concurrent disk I/O available on your SQL Server and can significantly increase performance.

> **NOTE:**
> Supported environments include those editions of SQL Server that support database partitioning and file groups (Enterprise editions of 2012, 2014, or 2016, and the Standard edition of SQL Server 2016 SP1).
>
> For more information on database partitioning, see your SQL Server documentation.

Benefits

It provides the following benefits to all ControlPoint database implementations, regardless of size:

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

  In addition to overall storage capacity requirement reduction, the storage structure of the databases is in smaller, more manageable files. This allows a systems operator to make use of smaller, more independent logical volumes.

- Reduces the storage throughput required for ControlPoint operations because it takes advantage of the concurrent storage channels/volumes usually available to production servers.
- Separates the structure of the database storage into multiple discrete files. This allows you to more accurately monitor your server for I/O hotspots while under load and to easily relocate component files to additional volumes.

  It 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. The major gain in this area is a reduction in necessary SQL index maintenance windows; allowing for more processing hours in a given day.

- Adds maintenance plans to all ControlPoint databases. The maintenance plans can be tailored by the 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.

For additional performance and stability guidelines, see the *ControlPoint Best Practices Guide.*

Recovery model for ControlPoint databases

With this release, the default recovery model for all ControlPoint databases is automatically set to SIMPLE.

If you wish to use either FULL or BULK-LOGGED, you can adjust it for each database after the installation is complete.

Install and configure SQL Server

To install SQL Server, follow the installation instructions provided by Microsoft.

> **NOTE:**
> To gain the best performance, Micro Focus recommends that you do not install any other ControlPoint components on the SQL Server.
>
> If you are deploying the ControlPoint databases to a server hosting other ControlPoint components, such as connectors, configure SQL Server to limit the resources it consumes.

For additional performance and stability guidelines, see the *ControlPoint Best Practices Guide.*

Configure the ControlPoint data source

Configure the ControlPoint data source in SQL Server Reporting Services 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.**

For more information, see step 10 of Install the ControlPoint databases, on page 21.

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

     For more information, see step 10 of Install the ControlPoint databases, on page 21.

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 ControlPoint MetaStore 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 ControlPointAudit databases.

Before you begin

Review the prerequisites

Review the prerequisites, including the scale and performance recommendations for the ControlPoint databases.

For more information, see Minimum hardware requirements - ControlPoint database server, on page 14 and Performance considerations, on page 18. Also see the *ControlPoint Best Practices Guide*.

Minimum SQL permissions

The user account that deploys or upgrades the ControlPoint databases must have permissions equivalent to the **sysadmin** default SQL login role.

This includes the permission to add, delete and modify jobs SQL Agent jobs, which requires access to the **msdb**. It also includes permission to examine database and filegroup structures, adding new ones as appropriate.

After deployment, the permissions of the SQL login account may be then reduced. The minimum required permissions for each of the ControlPoint databases' user is **db_owner**.

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.

Read and write permissions on paths

The desired paths to place the database file groups must be granted read and write permission appropriately.

This includes standard permissions on the objects and UAC access (usually controlled by ownership inheritance) if applicable.

These are the minimum permissions and access controls required to the directory targets, further additional access to the directories is of course permitted.

- When utilizing a SQL user account, these directories need to have read and write access (and UAC access) granted to both the user account running the database installation program on the SQL server and the user account that is being used to operate the SQL Server instance.
- When utilizing a Windows user account, these directories need to have read and write access (and UAC access) granted to the user account being used to run the installation program.

Local volumes for database files

The volumes you use for the ControlPoint database files must be local to the server where SQL Server is installed. This is a SQL Server requirement.

Logical file groups and the ControlPoint database installation program

The installation of the ControlPoint databases 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 corresponding to 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.

If desired, these individual files can be further moved by the Database Administrator after database creation to any other storage targets to further spread and control the SQL I/O utilization.

In addition, the installation program provides the ability to optionally 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.

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.

Install the ControlPoint databases

To install ControlPoint databases

1. Run `ControlPoint Database Installer.exe` as the Administrator.

   The file is located in the `ControlPoint x64\` directory.

   > **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 create databases and sufficient permission to the database file locations.

   The database installer opens.

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** name, or select them from the list.

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

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

6. The option to **Enable interleaving for database transactions** is selected by default.

   This option 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.

   > **NOTE:**
   > If only one disk is present, deselect the option.

7. Click **Test Connection** to verify the server details.

8. In the **Job Owner Username** box, enter a SQL Server username 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 validate for it.
   >
   > For more information on the maintenance jobs, see Next steps, on page 30.

9. Click **Next**.

   The ControlPoint Database Configuration page opens.

   For each setting, specify the path, or click the browse button to define the path.

   > **NOTE:**
   > The volumes you use for the ControlPoint database files must be local to the server where SQL Server is installed.

   > **NOTE:**
   > If you selected the option to interleave database transaction interleaving in step 6, the page indicates the paths participating in the interleaving.

   - **Data File.**

   - **Index File.**

> **NOTE:**
> Micro Focus recommends that the Index files be on a different volume from the other components in the file group.

- **Text File.**
- **Data Analysis Data.**
- **Data Analysis Text.**
- **Log file.**

> **NOTE:**
> For each database, configure the database log file to exist on a different volume than the database files.

Click **Next.**

The ControlPoint Audit Database Configuration page opens.

10. For each setting for the ControlPoint Audit database, specify the path, or click the browse button to define the path.

> **NOTE:**
> The volumes you use for the ControlPoint database files must be local to the server where SQL Server is installed.

> **NOTE:**
> If you selected the option to interleave database transaction interleaving in step 6, the page indicates the paths participating in the interleaving.

- **Data File.**
- **Index File.**
- **Text File.**
- **Log file.**

Click **Next.**

The ControlPoint Tracking Database Configuration page opens.

11. For each setting for the ControlPoint Tracking database, specify the path, or click the browse button to define the path.

> **NOTE:**
> The volumes you use for the ControlPoint database files must be local to the server where SQL Server is installed.

> **NOTE:**
> If you selected the option to interleave database transaction interleaving in step 6, the page indicates the paths participating in the interleaving.

- **Data File.**
- **Index File.**
- **Text File.**
- **Log file.**

  Click **Next.**

  The ControlPointMetaStore Database Configuration page opens.

12. For each setting for the ControlPoint MetaStore database, specify the path, or click the browse button to define the path.

> **NOTE:**
> The volumes you use for the ControlPoint database files must be local to the server where SQL Server is installed.

> **NOTE:**
> If you selected the option to interleave database transaction interleaving in step 6, the page indicates the paths participating in the interleaving.

- Data File.
- Index File
- Text File
- Metadata Data
- Metadata Index
- Metadata Text
- Metastore Data
- Metastore Index
- Metastore Text
- Metastore LDC Data
- Metastore LDC Index
- Metastore LDC Text
- Metastore Pro Data
- Metastore Pro Index
- Metastore Pro Text
- MS LDC Cache Data
- MS LDC Cache Index
- MS LDC Cache Text

- **Log file.**

  Click **Next.**

  The ControlPointMetaStoreTags Database Configuration page opens.

13. For each setting for the ControlPoint MetaStoreTags database, specify the path, or click the browse button to define the path.

    > **NOTE:**
    > The volumes you use for the ControlPoint database files must be local to the server where SQL Server is installed.

    - **Data File.**
    - **Index File.**
    - **Text File.**
    - **Log file.**

    Click **Next.**

14. The ControlPoint Audit Reports page opens.

15. To upload audit reports to SQL Server Reporting Services (SSRS), select **Upload Reports** and click **Next**.

    > **NOTE:**
    > This step requires that a data source in SQL Server Reporting Services was configured as a prerequisite. For more information, see Configure the ControlPoint data source, on page 22.

    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** box.

    b. In the Report Manager Server Settings area, enter the following information:

       i. **Report Manager URL.**

       ii. **Report Manager Virtual Directory.**

       > **NOTE:**
       > These settings are defined in the SQL Server Reporting Services Configuration Manager on the **Report Manager URL** tab. See step 5 of Configure the ControlPoint data source, on page 22.

       iii. **Report Webservice Virtual Directory.**

       > **NOTE:**
       > This is the virtual directory defined in the SQL Server Reporting Services Configuration Manager on the **Web Service URL** tab. See step 4 of Configure the ControlPoint data source, on page 22.

16. Click **Next**.

17. 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 to abort the execution, 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 **temp_db** database.
    >
    >   Dropping the databases avoids inconsistencies resulting from incomplete script executions.
    >
    > d. Restart the database installation program.

18. Review the installation log.

19. Click the hyperlink to copy the connection string to your clipboard. The ControlPointMetaStore service requires this connection string to access the ControlPointMetaStore database.

    Save this connection string for configuring your ControlPoint IDOL package in step 14 of Configure deployment packages, on page 33.

20. Click **Finish**.

    The installation wizard closes.

Next steps

After the database installation completes, do the following:

1. Verify the new SQL maintenance jobs.

2. If you did not install the **ControlPointMetaStore** and **tempDB** databases on dedicated hard drives, ensure that each is moved to their own dedicated hard drive. For example, **ControlPointMetaStore** is located on its own dedicated drive and **tempDB** is located on its own dedicated drive.

Verify the new SQL maintenance jobs

To verify the jobs

- In SQL Server Management Studio, navigate to **SQL Server Agent > Jobs** to verify the existence of ControlPoint database maintenance jobs.

  For each ControlPoint database, two maintenance jobs are created:

- **<databaseName>_db_maint_3.0.** The database maintenance job that by default, runs automatically at 10 pm every night.
- **<databaseName>_db_maint_all.** The database maintenance job that you can run manually as needed.

where

<databaseName> is the name of the ControlPoint database.

For example:

ControlPoint_db_maint_3.0 and ControlPoint_db_maint_all

> **NOTE:**
> The **_all** version of the maintenance script does not have a schedule defined, as it is intended to be run manually.

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://msdn.microsoft.com/en-us/library/ms345483(v=sql.120).aspx.

Example

This example describes the process of moving 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:**
   > **TempDB** 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**.

Chapter 4: Install ControlPoint IDOL and connectors

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

- Overview
- Create deployment packages
- Install deployment packages
- Uninstall deployment packages
- Deploy multiple MetaStore services

Overview

To install ControlPoint IDOL and connectors

1. Create deployment packages for the target servers. See Create deployment packages, below.
2. Copy the deployment packages to the target servers and install them. See Install deployment packages, on page 37.

Create deployment packages

The ControlPoint IDOL Deploy Tool automates the creation of deployment packages for ControlPoint IDOL and connectors. The Deploy 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.

The Deploy Tool configures the Deployment packages and the software requires no further configuration for use with ControlPoint after the installation on target servers.

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

Use the Deploy Tool to configure, save, and build deployment packages.

Configure deployment packages

Use the information in this section to configure 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.

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

     The default location is:

     `C:\Program Files\Micro Focus\ControlPoint\`.

   - **Zip File**. This option outputs the deployment packages as compressed (zip) archives.

     This option is useful when the deployment packages are to be transferred to different servers. The package size can exceed 1 GB.

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

     The default location is:

     `C:\temp\ControlPoint\`.

   - **Host Operating System**. Displays the architecture of the host operating system.

   - **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**.

4. On the **Connectors** tab, select the connectors to deploy. Click **Config** to configure each connector.

   The connector configuration dialog box opens. The information you provide depends on the type of connector.

   - Exchange (the client is installed on the server hosting the connectors)
   - File System
   - Hadoop
   - Notes

     > **NOTE:**
     > The Notes client software must be installed on the server hosting the ControlPoint Notes Connector.

   - SharePoint Remote
   - Documentum
   - Content Manager

     > **NOTE:** The Content Manager client software must be installed on the server hosting the ControlPoint Content Manager Connector. See Prerequisites, on page 13.

   a. (*Optional*) For an Exchange Connector, enter the following information.

      - **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.

   b. (*Optional*) For a File System Connector, enter the following information.

      - **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.

   c. (*Optional*) For a Hadoop Connector, enter the following information.

- **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.

d. (*Optional*)For a Notes Connector, enter the following information.

- **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.

e. (*Optional*) For a SharePoint Remote Connector, enter the following information.

- **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.

f. *(Optional)* For a Content Manager Connector, enter the following information.

   i. **Number of Connectors in Group**. Enter the number of connectors in the group. The maximum number is 9.

   ii. **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.

g. *(Optional)* For a Documentum Connector, enter the following information.

   i. **Number of Connectors in Group**. Enter the number of connectors in the group. The maximum number is 9.

   ii. **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.

   iii. **Documentum Hosts**. Enter the name of the Documentum server.

iv. **Documentum Credentials Username**. Enter the name of the user to use when authenticating with the Documentum server..

v. **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.

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 saved or copied to clipboard in step 13 of Install the ControlPoint databases, on page 21. 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

To save all configuration settings to a file, select **Save** or **Save As** from the File menu.

Build deployment packages

To build deployment packages, click **Deploy**, or select **Deploy** from the Actions menu. The packages are built in the Host Package Build Location that you specified on the **General** tab of the Deploy Tool.

Install deployment packages

The Deploy Tool creates deployment packages in the location identified by the **Host Package Build Location** option.

At this location are directories or compressed (.ZIP) files for each target server. Move the directories or .ZIP files to the appropriate target servers for installation.

Prerequisites

Prerequisite software

The following products must be installed on the target servers:

- Microsoft Visual C++ 2005 Redistributable Package
- Microsoft Visual C++ 2010 Redistributable Package
- Microsoft Visual C++ 2013 Redistributable Package
- SQL Native Client

The required prerequisite packages are included in the `vcredist` and `sqlNativeClient` subdirectories under the deployment package location.

IDOL license key

To use IDOL, you must have a valid license key file for the products that you want to use. Contact Micro Focus Support to request a license file for your installation.

The IDOL license key file must be copied to the IDOL License Server. For more information, see step 4 of Installation.

Installation

Perform the procedure in this section to install deployment packages.

To install a deployment package

1. Run the `_deploy_services.bat` Windows batch file as the local administrator of the server.

   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. Run the `_install_services.bat` Windows batch 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 ControlPoint MetaStore service.

   Enter the required username and password.
6. Copy the IDOL license file to the IDOL License Server directory after installation and before services start.
   a. 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
      ```

IDOL Content language type setup

By default, 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.

Start Windows services

To start all of the Windows services, run the `_start_services.bat` Windows batch file as the local administrator of the server.

> **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 identified when the connectors were configured in the Deploy Tool.

Stop Windows services

To stop all Windows services, run the `_stop_services.bat` Windows batch file.

To stop individual components in isolation, run `_stop_service.bat` in the component directory.

Deploy multiple MetaStore services

To enhance the ingestion performance of ControlPoint, you can deploy multiple MetaStore service components. The primary MetaStore component is dedicated to control operations; additional MetaStore nodes are devoted to ingestion of documents and policy execution.

The primary MetaStore component is deployed during installation; it is a manual process to deploy any additional MetaStore service nodes. You should deploy the additional MetaStore components after all other IDOL and connectors have been deployed.

Having a single Connector with its own MetaStore for ingestion results in the best ingestion performance.

Before you begin

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>\MetaStore`**`2`**

   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 `MetaStore`**`2`** 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 MetaStore**2** component, navigate to 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 MetaStore**2.**

   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 Metastore**2**:

   ```
   "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 the `_start_service.bat` in a text editor.
3. Update all service names from Metastore to Metastore**2**:

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

4. Save the file.

Modify the Stop Services script

1. Open the `_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 directory:

   ```
   \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 manually uninstall deployment packages, run the `_uninstall_services.bat` script.

To uninstall individual components, run `_uninstall_service.bat` in the component directory.

Chapter 5: Install ControlPoint components

This chapter describes how to install ControlPoint components.

- Federal Information Processing Standards (FIPS) security mode
- Install ControlPoint and the ControlPoint Engine
- Configure ControlPoint

Federal Information Processing Standards (FIPS) security mode

The Federal Information Processing Standard (FIPS) is a United States government standard specify 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.

Before you begin

> **NOTE:**
> If you do not use FIPS in your ControlPoint environment, ignore this section.

If you want to install ControlPoint on FIPS-enabled Windows servers, enable FIPS on the servers before you install and deploy ControlPoint.

For more information, see your Windows documentation on enabling FIPS encryption.

You use the ControlPoint Configuration Manager to enable the use of FIPS in your ControlPoint environment. For more information on the configuration process, see Step 10 of Configure ControlPoint, on the next page

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.

Install ControlPoint and the ControlPoint Engine

Before you install ControlPoint and the ControlPoint Engine, verify that the ControlPoint prerequisites listed in Prerequisites have been met.

To install ControlPoint Console and Engine

1. Run `setup.exe` as the Administrator.

   The file is located in the `ControlPoint x64\` 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

The ControlPoint Configuration Manager allows you to configure the ControlPoint system centrally.

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

Before you begin

The following configuration procedure assumes that you are configuring the Content Manager environment on one server.

To configure ControlPoint

> **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**.

1. Launch the ControlPoint Configuration Manager.

   The Configuration Manager opens.

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 web site 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.

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. Specify whether to enable Advanced IDOL Mode by clicking **Enable Advanced IDOL Mode**.

    j. In the MetaStore Service Settings section, enter the **MetaStore Host** name and **Port** number.

10. On the **Security** settings tab, specify options for enabling security:

    - Specify whether to enable ControlPoint security by clicking **Enable Security**.

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

      > **NOTE:**
      > If you plan to enable security in ControlPoint, 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**.

    > **NOTE:**
    > 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.

> **NOTE:**
> After FIPS is enabled as the security mode and the ControlPoint environment is deployed, the FIPS security mode cannot be changed. For more information, see Federal Information Processing Standards (FIPS) security mode

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

    - **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* or the Administration Console Help system.

12. 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.

Create a decoupled IDOL database repository

Creating a decoupled IDOL database repository involves updating config files to define the repository configuration, and then enabling it either through the ControlPoint web application or command-line utility.

> **NOTE:**
> You can create a decoupled IDOL database only from a new repository. You cannot edit an existing repository to create a decoupled IDOL database repository.

Before you begin

You must have enabled **Advanced IDOL Mode** in ControlPoint Configuration Manager before creating a decoupled IDOL database repository, as described in Configure ControlPoint, on page 44. You cannot create a decoupled IDOL database repository while in normal mode.

To create a decoupled IDOL database repository

1. 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 `[Databases]` section, increment the existing number of databases and add the new IDOL database.

      For example, in a file with two databases, add a third one, as shown in bold:

      ```
      [Databases]
      NUMDBS=3   <--increment
      0=News
      1=Archive
      2=NEW_IDOL_DATABASE   <--add
      ```

   c. Save the file.

2. Define a new visual database that maps to the new IDOL database.

   a. Open the `C:\Program Files\Micro Focus\ControlPoint\Indexer\IDOL\ControlPoint IDOL.cfg` file in a text editor.

   b. Increment the number of virtual databases, and then add a new one that maps to the database.

      For example, in a file with two existing virtual databases, define a third one, as shown in bold:

      ```
      VirtualDatabases=3  <--increment
      [vdb0]
      DbName=News
      Internal=False
      Type=combinator
      MapsTo=0:News

      [vdb1]
      DbName=Archive
      Internal=False
      Type=combinator
      MapsTo=0:Archive

      [vdb2]  <-- add
      DbName=NEW_IDOL_DATABASE
      Internal=False
      Type=combinator
      MapsTo=0: NEW_IDOL_DATABASE
      ```

   c. Save the file.

3. In Windows Servcies Manager, manually restart the **ControlPoint IDOL** and **ControlPoint Content** services.

4. Run the following queries to verify the database was created successfully:

   - `http://localhost:9000/a=getstatus`
   - `http://localhost:32000/a=getstatus`
   - `https://localhost/ControlPoint/RepositoryManagement/GetIdolDatabase`
   - `https://localhost/ControlPoint/RepositoryManagement/GetAdvancedIdolMode`

   For the first three queries: If you notice a problem, verify your updates to the `ControlPoint Content.cfg` and `ControlPoint IDOL.cfg` files. You must use the same name in both files and it must be different than any existing name.

   For the fourth query: The result should indicate that advanced mode is `true`. If not, verify that you selected it, as described in Configure ControlPoint, on page 44.

5. To enable the decoupled IDOL database through the ControlPoint web application:

   a. On the **REPOSITORIES** tab of the application, click **New Repository**.

   b. In the **NAME** field of the **DETAILS** section, enter the same name for the IDOL database (***NEW_IDOL_DATABASE***) that you specified in the `ControlPoint Content.cfg` and `ControlPoint IDOL.cfg` files.

   c. In the **ANALYSIS** section, do the following:

      - For **ANALYSIS TYPE**, click **Content**.
      - In the **IDOL DATABASE** list, select the database you specified in the **DETAILS** section.

   d. Click **Save**.

6. To enable the decoupled IDOL database using the ControlPoint command-line utility:

   a. Create a copy of the sample XML file provided in the `ControlPoint\<`*`version`*`>\Utilities\CommandLine Utility\Sample` folder that matches your repository type.

      For example, for an Microsoft Exchange repository, copy the `Repository_CP_Exch.xml` file.

   b. Open your copy of the file in a text editor, and do the following:

      i. Locate the `<name>` and `<idol_database>` entries, and then change the sample repository name to the one you specified in the configuration files. The name is case-sensitive.

         For example, for a file based on `Repository_CP_Exch.xml`, update the following lines and replace `Exch_Repo_1` with the name of your IDOL database repository:

         - `<name>Exch_Repo_1</name>`
         - `<idol_database>Exch_Repo_1</idol_database>`

      ii. Locate the `<analysis_type>` entry and change it from:

         `<analysis_type>`**`Metadata_Only`**`</analysis_type>`

         to

         `<analysis_type>`**`Content`**`</analysis_type>`

c. Save the file.

d. Open a Command Prompt window. At the prompt, enter the following command to create the repository:

```
ControlPointCommand.exe -action repo_create -config_path <XMLfile> -report_
path <reportFile> -enablehttps 0
```

Where:

- `XMLfile` is the name of the XML file you updated.
- `reportFile` is the name of the report the utility creates.

For example, the following command creates a decoupled IDOL database repository based on information in the `C:\temp\myRepo.xml`:

```
ControlPointCommand.exe -action repo_create -config_path C:\temp\myRepo.xml
-report_path C:\report -enablehttps 0
```

Deploy ControlPoint by enabling HTTPS

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

- Enable HTTPS
- Redeploy ControlPoint when HTTPS is enabled
- Enable ControlPoint workflow capability with ControlPoint HTTPS deployment (optional)

Enable HTTPS

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

1. Create a Certificate Authority to sign the server and client certificates. These certificates must be added to the certificate stores. See Create certificates.
2. Configure applications in IIS to require the certificates. See Configure certificates in IIS Manager.
3. Update the required Web configuration files. See Update the 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.

Complete the following tasks:

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 certificates in IIS Manager

Add the certificates to IIS Manager and configure bindings and app 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 update the bindings

1. In the IIS Manager, from the navigation pane on the left, select the web site.
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 the 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` comment.
4. Update the host in the endpoint addresses if necessary.
5. In the `clientCertificate` tag, 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.

   > **CAUTION:** Enter this value manually. Do not copy and paste this value from the certificate, as the encoding adds hidden characters that will cause issues.

   > **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

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` comment.

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` comment.
4. Update the host in the endpoint addresses, if necessary.
5. In the `clientCertificate` tag, 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` comment.
4. Update the host in the endpoint addresses if necessary.
5. In the `clientCertificate` tag, 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 Dashboard, Timer, and WebService `web.config` file in the **https** service section.

Enable ControlPoint workflow capability with ControlPoint HTTPS deployment (optional)

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. Copy the `system.serviceModel -> bindings -> basicHttpBinding -> SOAPManagerIFV3PortSoapBinding` binding block from the HTTP service model in the same `app.config` file to the HTTPS service model.

5.6.0.140\ControlPoint\5.6.0\ControlPoint Database Installer.exeConfigure 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.

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

Limitations

ControlPoint has the following limitations when using URL redirection:

- Shortcut redirect to the new location supports only IE browser.

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.

Complete the following tasks:

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

Bind the created certificate to Redirector service port 7050.

1. Open PowerShell and run the following command:

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

   Example

   ```
   netsh http add sslcert ipport=10.10.10.1:7050
   certhash=6b58bff0b663d452a32bdcdff4ba72ba8f18ce79 appid={4f3f8d5c-c5a9-4ecc-85fb-b17db658f246}
   ```

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

Redirector service HTTPS configuration

To edit the Redirector service configuration file

1. Navigate to : `\Program Files\Micro Focus\ControlPoint\Engine\Scheduler\ControlPointTimer.exe.config` and add the following parameter.

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

   Set the parameter to `"true"` for HTTPS.

2. Save the file.
3. Navigate to `Program Files\Micro Focus\ControlPoint\Engine\Redirector.exe.config` file and add the following parametes.

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

   Set the parameters to `"true"` for HTTPS.
4. Save the file.
1. Restart the Redirector service and ControlPoint Engine service.

Chapter 6: Install ControlPoint Edge Filesystem connector

This section provides information on installing the ControlPoint Edge Filesystem connector. The Edge Filesystem connector is used to run Archive policies on documents and files held in Windows and Linux file shares.

- Prerequisites
- Install the Edge Filesystem connector
- Edge Filesystem Connector configuration file
- Upgrade the Edge Filesystem connector
- Uninstall the Edge Filesystem connector

Prerequisites

Component	Description
Platform	**Windows:** • Windows 2012 R2 Server or later. • Windows 2016 Server or later. **Linux:** • RHEL 7.2 • SUSE 12
ControlPoint	Installed and ready to use.

Install the Edge Filesystem connector

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

To install the ControlPoint Edge Filesystem Connector on Windows

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

   You can find the installer at `ControlPoint x64\ControlPoint \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 Filesystem 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 Filesystem 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. Click **Next**.

   The Service User page opens.

9. Specify the credentials that will be used to run the ControlPoint Edge Filesystem Connector services and to connect to the ControlPoint server.

10. Click **Next**.

    The Installation Confirmation page opens.

11. Click **Install**.

    After the connector is installed, you are prompted to restart the system to complete the installation.

To install the ControlPoint Edge Filesystem Connector on Linux

1. Open the Edge Filesystem Connector ports: 7210 and 7212.

2. Run the ControlPoint Edge Filesystem Connector, `SORHELInstall.tar.gz`.

   You can find the installer at `ControlPoint x64\ControlPoint\ Agents\ControlPoint File System Agent\Red Hat Linux`

   or

   `ControlPoint x64\ControlPoint\ Agents\ControlPoint File System Agent\SUSE Linux`.

3. Extract and install the tarball as follows:

   a. `tar -xvzf SORHELInstall.tar.gz`

   b. `cd SORHELInstall`

   c. `sh sosetup.sh install`

4. Create a mount directory using the following command:

   ```
   mkdir /opt/mount
   ```

5. Run the configuration scripts that configure and start the services as follows:

a. `sh /opt/Micro\ Focus/Edge/Agent/resources/deployLoggedFS.sh`

   When prompted, enter the mount location created in Step 3.

b. `sh /opt/Micro\ Focus/Edge/EdgeFSConnector/deployFSConnector.sh`

   i. When prompted, enter the ControlPoint server, domain, username, and password.

   ii. When prompted, specify whether or not to use enable HTTPS:

   - Enter **y** for ControlPoint environments running with HTTPS.
   - Enter **n** for environments running with HTTP.

Edge Filesystem Connector configuration file

The Edge Filesystem Connector configuration file for Windows and Linux has a new config section "EnableSSL", which is disabled by default.

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

If IDOL on the ControlPoint server is already using HTTPS, the Edge Filesystem Connector should also use HTTPS in order to be listed on the connection list on the Repository page in the ControlPoint Dashboard.

All other HTTPS configurations to run the Edge Filesystem Connector on HTTPS are similar to the configuration on a regular Filesystem connector.

Uninstall the Edge Filesystem connector

To uninstall the ControlPoint Edge Filesystem Connector on Windows

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

To uninstall the ControlPoint Edge Filesystem Connector on Linux

1. Change the directory to the `SORHELInstall` directory and run the following command: `sh sosetup.sh remove`
2. Stop the `EdgeConnectorFramework.exe` process or reboot the system.

Chapter 7: Optimize IDOL configuration

> **NOTE:**
> This is applicable to ControlPoint Content only. 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*.

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`	Use this parameter to reduce the analysis size and RAM consumption, which will speed up analyzing. Set `SplitNumbers` to `False` if you need numeric wild card searching. **Example:** `SplitNumbers=false`
`FlushLockFile`	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. **Example:** `FlushLockFile=\\host1\Lock\SanLockFileHost1.txt` 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. 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.

`IndexCacheMaxSize`	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.
	Example:
	`[IndexCache]`
	`IndexCacheMaxSize=102400`
	Setting the `IndexCacheMaxSize` option requires knowledge of the

Parameter	Description
	system. • If IndexCacheMaxSize is too small, indexing becomes slow. • 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 8: HTTPS setup for IDOL

This section provides information on the following:

- Set up HTTPS for IDOL and connectors
- Stop IDOL services running with HTTPS
- Run the ControlPoint Configuration Manager with HTTPS enabled
- Troubleshooting

Set up HTTPS for IDOL and connectors

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

- Create SSL certificates in the environment. See Create SSL certificates.
- Update the IDOL configuration. See Update the IDOL configuration.
- Optionally, enable TLS 1.2 protocol. See Enable TLS 1.2 protocol, on page 70
- Enable IDOL in HTTPS mode. See ControlPoint settings to enable IDOL in HTTPS mode.

Create 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.

1. Stop the IDOL, Connector and, ControlPoint related services. This can be done in either of the following ways:

   a. Run `_stop_service.bat`, which is located in the `temp` directory present in the installation path (`\temp\ControlPoint\host_<HOSTNAME>`)

   or

   b. Using Services, manually stop the services in the following order:

      - FileSystem Connector
      - FileSystem Connector Framework

   - Distributed Connector
   - SharePoint Remote Connector
   - SharePoint Remote Connector Framework
   - MetaStore
   - IDOL
   - OGS
   - Statistics
   - Content
   - LicenseServer

2. Modify the configuration (`.cfg`) files located in the installation directory.

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

   The default or generic configuration files are:

   - `ControlPoint IDOL.cfg`
   - `ControlPointContent.cfg`
   - `ControlPointDistributed Connector.cfg`
   - `ControlPointFileSystem Connector.cfg`
   - `agentstore.cfg`
   - `ControlPoint Filesystem Connector Framework.cfg`
   - `ControlPoint DataAnalysis Store.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 `File System connector.cfg` file.

   ### ControlPoint IDOL.cfg

   a. Navigate to: `\Program Files\Micro Focus\ControlPoint\Indexer\IDOL` and open `ControlPoint IDOL.cfg`.

   b. Add the location of the server certificate and server key:

   ```
   [SSLOption0]
   SSLMethod=SSLV23
   SSLCertificate=<location>\server.crt
   SSLPrivateKey=<location>\server.key
   ```

   [Server] section

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

[Service] section

```
Add SSLConfig=SSLOption0
```

[DataDRE] section

```
Add SSLConfig=SSLOption0
```

[CatDRE] section

```
Add SSLConfig=SSLOption0
```

[AgentDRE] section

```
Add SSLConfig=SSLOption0
```

[Viewing] section

```
Add SSLConfig=SSLOption0
```

[IndexServer] section

```
Add SSLConfig=SSLOption0
```

[Agent] section

```
Add SSLConfig=SSLOption0
Add 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

```
Add SSLConfig=SSLOption0
```

[DIHEngine0] section

```
Add SSLConfig=SSLOption0
Add ServiceSSLConfig=SSLOption0
```

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

ControlPoint Content.cfg

a. Navigate to: `\Program Files\Micro Focus\ControlPoint\Indexer\Content` and open `ControlPoint Content.cfg`.

b. Add the location of the server certificate and server key:

```
[SSLOption0]
SSLMethod=SSLV23
SSLCertificate=<location>\server.crt
```

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

[Server] section

```
Add SSLConfig=SSLOption0
```

[Service] section

```
Add SSLConfig=SSLOption0
```

[IndexServer] section

```
Add SSLConfig=SSLOption0
```

ControlPoint Distributed Connector.cfg

a. Navigate to: `\Program Files\Micro Focus\ControlPoint\Indexer\Distributed Connector` and open `ControlPoint Distributed Connector.cfg`.

b. Add the location of the server certificate and server key :

```
[SSLOption0]
SSLMethod=SSLV23
SSLCertificate=<location>\server.crt
SSLPrivateKey=<location>\server.key
```

[Server] section

```
Add SSLConfig=SSLOption0
```

[Service] section

```
Add SSLConfig=SSLOption0
```

[IndexServer] section

```
Add SSLConfig=SSLOption0
```

[Idol] section

```
Add SSLConfig=SSLOption0
```

[Fetch] section

```
Add SSLConfig=SSLOption0
```

[DistributedConnector] section

```
Add ConnectorSSLConfig=SSLOption0
Add SSLConfig=SSLOption0
```

ViewServer section

```
Add SSLConfig=SSLOption0
```

ControlPoint xxx Connector.cfg

a. Navigate to: `\Program Files\Micro Focus\ControlPoint\Indexer\xxx Connector\ControlPoint xxx Connector.cfg`

   where

   `xxx` is the Connector name.

b. Add the location of the server certificate and server key:

```
[SSLOption0]
SSLMethod=SSLV23
SSLCertificate=<location>\server.crt
SSLPrivateKey=<location>\server.key
```

   Server section

   `Add SSLConfig=SSLOption0`

   Service section

   `Add SSLConfig=SSLOption0`

   IndexServer section

   `Add SSLConfig=SSLOption0`

   Fetch section

   `Add SSLConfig=SSLOption0`

   ViewServer section

   `Add SSLConfig=SSLOption0`

   FetchTasks section

   `Add SSLConfig=SSLOption0`

   DistributedConnector section

   `Add SSLConfig=SSLOption0`

   Ingestion section

   `Add IngestSSLConfig=SSLOption0`

   Connector section

   `Add IngestSSLConfig=SSLOption0`

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

ControlPoint xxx Framework.cfg

a. Navigate to: `\Program Files\Micro Focus\ControlPoint\Indexer\xxx Connector Framework\ControlPoint xxx Framework.cfg`

   where `xxx` is the connector.

b. Add the location of the server certificate and server key :

   ```
   [SSLOption0]
   SSLMethod=SSLV23
   SSLCertificate=<location>\server.crt
   SSLPrivateKey=<location>\server.key
   ```

   Server section

   ```
   Add SSLConfig=SSLOption0
   ```

   Service section

   ```
   Add SSLConfig=SSLOption0
   ```

   MyIdolIndexer section

   ```
   Add SSLConfig=SSLOption0
   ```

   Categorizer section

   ```
   Add SSLConfig=SSLOption0
   ```

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

c. 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\Micro 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 = "SSLV23",
    }
   ```

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.

agentstore.cfg

a. Navigate to: `\Program Files\Micro Focus\ControlPoint\Indexer\IDOL\agentstore\agentstore.cfg`.

b. Add the location of the server certificate and server key:

```
[SSLOption0]
SSLMethod=SSLV23
SSLCertificate=<location>\server.crt
SSLPrivateKey=<location>\server.key
```

[Server] section

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

[Service] section

```
Add SSLConfig=SSLOption0
```

ControlPoint DataAnalysis Store.cfg

a. Navigate to : `\Program Files\Micro Focus\ControlPoint\Indexer\Statistics\ControlPoint DataAnalysis Store.cfg`

b. Add the location of server certificate and server key :

```
[SSLOption0]
SSLMethod=SSLV23
SSLCertificate=<location>\server.crt
SSLPrivateKey=<location>\server.key
```

[Server] section

```
Add SSLConfig=SSLOption0
```

[Service] section

```
Add SSLConfig=SSLOption0
```

[IndexServer] section

```
Add SSLConfig=SSLOption0
```

ControlPointOGS.cfg

a. Navigate to: `\Program Files\Micro Focus\ControlPoint\Indexer\OGS\ControlPoint OGS.cfg`

b. Add the location of server certificate and server key:

```
[SSLOption0]
SSLMethod=SSLV23
SSLCertificate=<location>\server.crt
SSLPrivateKey=<location>\server.key
```

[Server] section

```
Add SSLConfig=SSLOption0
```

[Service] section

```
Add SSLConfig=SSLOption0
```

Default section

```
Add GroupServerSSLConfig=SSLOption0
```

ControlPoint MetaStore.cfg

a. Navigate to: `\Program Files\Micro Focus\ControlPoint\Indexer\metaStore\ControlPoint metastore.cfg`

b. Add the location of server certificate and server key:

```
[SSLOp[SSLOption0] SSLMethod=SSLV23 SSLCertificate=<location>\server.crt
SSLPrivateKey=<location>\server.key
```

[Server] section

```
Add SSLConfig=SSLOption0
```

[Service] section

```
Add SSLConfig=SSLOption0
```

[IndexServer] section

```
Add SSLConfig=SSLOption0
```

[Actions] section

```
Add SSLConfig=SSLOption0
```

```
[IngestAction] section

Add SSLConfig=SSLOption0
```

3. In order to make MetaStore working in SSL mode, you must remove the following:

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

   and update the configurations in the `appSettings` section of the following files:

   ```
   ControlPointTimer.exe.config (..\Program Files\Hewlett Packard
   Enterprise\ControlPoint\Engine\Scheduler)

   Web.config (..\Program Files\Hewlett Packard Enterprise\ControlPoint\Dashboard)

   Web.config (..\Program Files\Hewlett Packard
   Enterprise\ControlPoint\Engine\CallBack)

   Web.config (..\Program Files\Hewlett Packard
   Enterprise\ControlPoint\DataAnalysis\Service)

   Web.config (..\Program Files\Hewlett Packard
   Enterprise\ControlPoint\WebService)

   Autonomy.ControlPoint.DataAnalysis.Controller.BundledAgent.exe.config
   (..Program Files\Hewlett Packard Enterprise\ControlPoint\DataAnalysis\Agent)

   Web.config (\Program Files\Hewlett Packard Enterprise\ControlPoint\Mvc)

   Autonomy.ControlPoint.DataAnalysis.Controller.BundledSqlAgent.exe.config
   (..\Program Files\Hewlett Packard
   Enterprise\ControlPoint\DataAnalysis\SqlAgent)
   ```

4. Start the IDOL, Connector and ControlPoint related services. This can be done in either of the following ways:

   a. Run `_start_service.bat`, which is located in the `temp` directory present in the installation path (`\temp\ControlPoint\host_<HostName>`)

   or

   b. Manually start the services in the following order:

      - LicenseServer
      - Content
      - Statistics
      - OGS
      - IDOL
      - Distributed Connector
      - FileSystem Connector Framework
      - FileSystem Connector
      - MetaStore

5. If there are any additional connectors or connector framework configuration files configured with SSL, then start them manually.
6. Restart the related services to access all ports securely.

Enable TLS 1.2 protocol

You can optionally enable the TLS 1.2 protocol for several ControlPoint connectors in your environment.

> **IMPORTANT:**
> Support for the TLS 1.2 protocol is limited to the Distributed Connector, Documentum Connector, SharePoint Remote Connector and the File System Connector only.

To enable TLS 1.2 support, configure the following components

1. Update the `\Program Files\Micro Focus\ControlPoint\Indexer\Distributed Connector\ControlPoint Distributed Connector.cfg` configuration file with the following settings (in bold):

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

   where

   for SSLMethod, the supported protocols are: SSLV23, TLSV1, TLSV1.1, or TLSV1.2.

2. Update the `\Program Files\Micro Focus\ControlPoint\Indexer\Documentum Connector\ControlPoint Documentum Connector.cfg` configuration file with the following settings (in bold):

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

   where

   for SSLMethod, the supported protocols are: SSLV23, TLSV1, TLSV1.1, or TLSV1.2.

3. Update the `\Program Files\Micro Focus\ControlPoint\Indexer\Documentum Connector Framework\ControlPoint Documentum Connector Framework.cfg` configuration file with the following settings (in bold):

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

   where, for SSLMethod, the supported protocols are: SSLV23, TLSV1, TLSV1.1, or TLSV1.2.

4. Update the `\Program Files\Micro Focus\ControlPoint\Indexer\SharePoint Remote Connector\ControlPoint SharePoint Remote Connector.cfg`. configuration file with the following settings (in bold):

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

   where, for SSLMethod, the supported protocols are: SSLV23, TLSV1, TLSV1.1, or TLSV1.2.

5. Update the `\Program Files\Micro Focus\ControlPoint\Indexer\SharePoint Remote Connector Framework\ControlPoint SharePoint Remote Framework.cfg` configuration file with the following settings (in bold):

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

   where, for SSLMethod, the supported protocols are: SSLV23, TLSV1, TLSV1.1, or TLSV1.2.

6. Update the `ControlPoint FileSystem Connector.cfg` configuration file with the following settings (in bold):

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

   where, for SSLMethod, the supported protocols are: SSLV23, TLSV1, TLSV1.1, or TLSV1.2.

7. Update the `ControlPoint FileSystem Connector Framework.cfg` configuration file with the following settings (in bold):

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

   where, for SSLMethod, the supported protocols are: SSLV23, TLSV1, TLSV1.1, or TLSV1.2.

ControlPoint settings to enable IDOL in HTTPS mode

1. Stop the application pool for the ControlPoint website in IIS.

2. Stop ControlPoint Engine in Services.

3. Configure the following ControlPoint settings to establish a secure connection to IDOL and the connector ports:

- The MetaStore port is specified in the ports.

  If the MetaStore port is customized or different, update the port:

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

- To specify the IDOL setup to use HTTPS mode, define the `"SecurePorts"` parameter to be true for `<add key="SecurePorts" value="true"/>` present in `<appSettings>`.

  For example:

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

- Change the configurations in the `appSettings` section of the following files:
  - `ControlPointTimer.exe.config` in `\Program Files\Micro Focus\ControlPoint\Engine\Scheduler`
  - `Web.config` in `..\Program Files\Micro Focus\ControlPoint\Dashboard`
  - `Web.config` in `..\Program Files\Micro Focus\ControlPoint\Engine\CallBack`
  - `Web.config` in `..\Program Files\Micro Focus\ControlPoint\DataAnalysis\Service`
  - `Web.config` in `..\Program Files\Micro Focus\ControlPointWebService`
  - `Autonomy.ControlPoint.DataAnalysis.Controller.BundledAgent.exe.config` in `..\Program Files\Micro Focus\ControlPoint\DataAnalysis\Agent`.

- In the `appSettings` section of the following configuration files, add the specified parameters:

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

  - `Web.config` in `\Program Files\Micro Focus\ControlPoint\Mvc`
  - `Autonomy.ControlPoint.DataAnalysis.Controller.BundledSqlAgent.exe.config` in `\Program Files\Micro Focus\ControlPoint\DataAnalysis\SqlAgent`

2. Start the ControlPoint website in IIS.
3. Start ControlPoint Engine in Services.
4. 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 enable IDOL in HTTPS mode 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 the ControlPoint Configuration Manager with HTTPS enabled

> **NOTE:**
> You can set up IDOL to use HTTPS and can have ControlPoint set up to use either HTTP or HTTPS.

If you configured all the IDOL components and connectors to work with HTTPS, then you must run the ControlPoint Configuration Manager, and 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**, then click **OK**.
5. Next, in the Certificates snap-in window select **Computer account** and 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. Navigate to:`\Program Files\Micro Focus\ControlPoint\Configuration.`

   Change the following configuration settings in the file, `ControlPointConfiguration.exe.config` in the `appSettings` section.

   ```
   <add key="SecurePorts" value="true" />
   ```
9. Launch the ControlPointConfiguration Manager and click **Deploy**.

Troubleshooting

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 can not 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 9: IDOLv distributed mirror / non-mirror setup

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

- Introduction
- Mirror mode setup
- Non-mirror simple combinator mode setup
- 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*.

Mirror mode setup

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.

Non-mirror simple combinator mode setup

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 2012 R2.
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, run the `_stop_service.bat` and `_uninstall_service.bat` batch files.

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

   `ControlPoint\ControlPoint 5.3.Utilities\Standlone DIH DAH`)

   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_XXX\Indexer` .
    - `langfiles` directory: `temp\ControlPoint\host_XXX\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	*

Section	Parameter	Value
[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	*

Section	Parameter	Value
[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 10: Upgrade ControlPoint

This chapter describes how to upgrade from a previous version of ControlPoint to version 5.6.1.

Overview of the upgrade process

The upgrade process consists of the following phases:

1. Verify that the environment is suitable for upgrade. See Before you begin.
2. Prepare the ControlPoint environment for upgrade. See Prepare the ControlPoint environment for upgrade.
3. Uninstall the current ControlPoint software. See Uninstall the ControlPoint software.
4. Upgrade ControlPoint to version 5.6.1:
   a. If you are upgrading from a release before 5.4, you must upgrade the databases to ControlPoint 5.4 before upgrading to 5.6.1. See Upgrade the ControlPoint databases to 5.4, on page 87.

   b. If you are upgrading from 5.4 to 5.5, see Upgrade the ControlPoint databases to 5.6.1, on page 88.

   c. After upgrade, for increased performance in the ControlPoint databases, Micro Focus strongly recommends that you run the database conversion packages included in your ControlPoint software build.

      - For more information on the benefits, see Database overview, on page 21 and Logical file groups and the ControlPoint database installation program, on page 24.
      - For detailed instructions on the database conversion process and associated downtimes, see the *ControlPoint Database Conversion Guide*.
5. For environments with Edge Filesystem connectors, upgrade the Edge Filesystem Connectors to 5.6.1. See Upgrade the Edge Filesystem connector .
6. After upgrade, update the Connector and Connector framework configuration file settings. For more information, see ControlPoint post-upgrade tasks.
7. After upgrade, integrate the IDOL proxy updates. For more information, see Integrate IDOL proxy updates , on page 103.

Before you begin

Ensure that your environment meets all hardware, software, and third-party component requirements as described in the Prerequisites section.

Run the Support Utility

For ControlPoint 5.4 release and later.

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

For more information, see ControlPoint Support utility, on page 158.

To gather environment information

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

   ```
   ControlPointSupportUtility.exe -c
   ```

   The utility gathers and copies all of the system information and configuration file information and label it as `Pre` capture data. It moves the data to the user's `\temp` directory for comparison.

   The locations of the `Pre` data files are as follows:

   ```
   <systemroot>\Users\<user>\AppData\Local\Temp\PreLogFiles
   ```

   ```
   <systemroot>\Users\<user>\AppData\Local\Temp\PostLogFiles
   ```

   ```
   <systemroot>\Users\<user>\AppData\Local\Temp\PreSystemInfo.xml
   ```

   ```
   <systemroot>\Users\<user>\AppData\Local\Temp\PostSystemInfo.xml
   ```

   > **NOTE:**
   > This information is used during a verification and comparison step after upgrade. See Post-upgrade steps, on page 107.

Prepare the ControlPoint environment for upgrade

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

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 the command:

   ```
   http://
   distributedconnectorhost:port/a=queueinfo&queuename=fetch&queueaction=getstatus
   ```

   If the Distributed Connector is working with HTTPS, check the queue by issuing the command:

   ```
   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:

   a. ControlPoint Engines

   b. Distributed Connector

   c. Individual connectors and Connector Framework Services.

      The services are stopped.

6. Back up the ControlPoint databases.

   - ControlPoint
   - ControlPoint Audit
   - ControlPointMetaStore
   - ControlPointMetaStore Tags
   - ControlPoint Document Tracking
   - ReportServer. Available if your environment is configured for reports.
   - ReportServerTempDB. Available if your environment is configured for reports.

7. Start the SQL Server Agent service.

   The SQL Server Agent service must be set to start automatically, and the service must be running.

Uninstall the ControlPoint software

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

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

   The software uninstalls.

> **NOTE:**
> For 5.4 ControlPoint environments, 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 fresh installation and you have the option to select or clear the **Enable FIPS security mode** checkbox.
> - 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 Federal Information Processing Standards (FIPS) security mode, on page 43.

2. Remove the ControlPoint Web sites.

   Identify all applications in the `ControlPointAppPool40` application pool running on your Internet Information Services (IIS) and remove them.

   a. Remove the ControlPoint Web sites.

      Identify all applications in the `ControlPointAppPool40` application pool running on your Internet Information Services (IIS) and remove them.

      Remove the ControlPointAppPool40

      It may include some or all of the following:

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

   b. Remove the `ControlPointAppPool40` application pool.

   The environment is ready for upgrade.

Upgrade to ControlPoint 5.6.1

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

The ControlPoint upgrade process consists of the following tasks.

1. Upgrade the ControlPoint databases.

   a. If you are upgrading from a release before 5.4, you must upgrade the databases to ControlPoint 5.4 before upgrading to 5.6.1. See Upgrade the ControlPoint databases to 5.4.

   b. If you are upgrading from 5.4 to 5.5, see Upgrade the ControlPoint databases to 5.6.1.

c. After the database upgrade, for increased performance in the ControlPoint databases, Micro Focus strongly recommends that you run the database conversion packages included in your ControlPoint software build.

   - For more information on the benefits of converting the databases to use database partitioning and file groups in SQL Server, see Database overview, on page 21 and ControlPoint databases and performance considerations, on page 96.

   - For detailed instructions on database conversion tasks and associated downtime, see the *ControlPoint Database Conversion Guide.*

2. Install the ControlPoint software, including optionally enabling HTTPS. See Install the ControlPoint software.

3. Verify the IDOL databases before upgrading the IDOL software. See Verify the databases in IDOL.

4. Upgrade IDOL data and software. See Upgrade IDOL data and software.

5. Upgrade the IDOL software manually. See Upgrade the IDOL software manually.

6. Update the connector and connector framework configuration files with settings from previous environment. See Update configuration files.

7. Update Content Manager configuration files with settings from Records Manager and TRIM connectors. See Update Content Manager Connector configuration files.

8. Perform additional post-upgrade tasks. See Post-upgrade steps.

Upgrade the ControlPoint databases to 5.4

> **IMPORTANT:**
> The following upgrade tasks apply only to environments being upgraded from releases prior to 5.4.
>
> If you are upgrading the ControlPoint environment from a release before 5.4, you must upgrade the databases to ControlPoint 5.4 before upgrading to 5.6.1.
>
> If your ControlPoint environment is already running 5.4, follow the tasks in Upgrade the ControlPoint databases to 5.6.1.

Obtain the ControlPoint 5.4 software

To obtain the ControlPoint 5.4 software package, download it from the following location:

https://downloads.autonomy.com/productDownloads.jsp

Alternately, the ControlPoint 5.4 Database Installer utility is available in the following location within the 5.6.1 software package.

```
ControlPoint\CP 5.5.Utilities\CP54DBInstaller\HPE ControlPoint 54
DatabaseInstaller.exe
```

Upgrade the ControlPoint databases to 5.4

To upgrade the ControlPoint databases

1. Navigate to the `\ControlPoint` directory in the 5.4 package and run `ControlPoint Database Installer.exe.`

2. Follow the instructions in the wizard.

   > **NOTE:** For upgrades from version 4.5 or earlier, two additional databases are created for ControlPoint 5.4:
   >
   > - ControlPointMetaStore
   > - ControlPointMetaStore Tags
   >
   > ControlPointMetaStore holds key metadata for all analyzed content and should be sized appropriately. Verify that the security settings in SQL Server are correct for these two databases.

   The databases are upgraded to the 5.4 release.

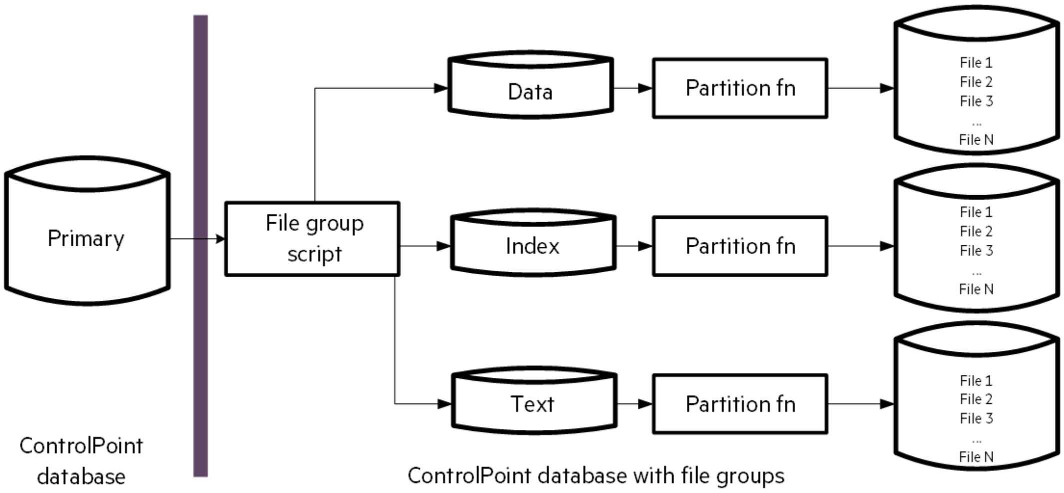
3. Proceed to Upgrade the ControlPoint databases to 5.6.1, below to upgrade the ControlPoint databases from 5.4 to 5.6.1.

Upgrade the ControlPoint databases to 5.6.1

For the 5.6.1 release of ControlPoint, Micro Focus has made performance improvements to the ControlPoint databases.

For more information on the benefits, see Database overview, on page 21.

The diagram below describes how each ControlPoint database is upgraded and separated into file groups for in the 5.6.1 release.



Recovery model for ControlPoint databases

With this release, the default recovery model for all ControlPoint databases is automatically set to SIMPLE.

If you wish to use either FULL or BULK-LOGGED, you can adjust it for each database after the upgrade is complete.

> **IMPORTANT:**
> The following tasks apply only to environments being upgraded from release 5.4 to 5.5.
>
> If you are upgrading the ControlPoint environment from a release before 5.4, you must upgrade the databases to ControlPoint 5.4 before upgrading to 5.6.1.
>
> See Upgrade the ControlPoint databases to 5.4.

Before you begin

Before you begin the upgrade of the ControlPoint databases, ensure that you have considered the following items.

Minimum SQL permissions

The user account that deploys and upgrades the ControlPoint databases must have 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.

> **IMPORTANT:**
> The user account must have permissions equivalent to the sysadmin default SQL login role. If you manually reduced permissions of this role, these permissions must be granted to the user account running the ControlPoint Database installation program.
>
> This includes permission to add, delete and modify jobs SQL Agent jobs, which requires access to the **msdb** database.
>
> - This may be a SQL user account, not a Windows account defined in SQL
>
>   or
>
> - This may be a Windows user account (explicitly assigned this role in SQL). If this option is chosen, the user account running the Database installer on the SQL server host must be this account.

Read and write permissions on paths

The desired paths to place the database file groups must be granted read and write permission appropriately.

This includes standard permissions on the objects and UAC access (usually controlled by ownership inheritance) if applicable.

These are the minimum permissions and access controls required to the directory targets, further additional access to the directories is of course permitted.

- When utilizing a SQL user account, these directories need to have read and write access (and UAC access) granted to both the user account running the database installation program on the SQL server and the user account that is being used to operate the SQL Server instance.
- When utilizing a Windows user account, these directories need to have read and write access (and UAC access) granted to the user account being used to run the installation program.

Upgrade the databases

To upgrade the 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.

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** name, or select them from the list.
5. Select the required authentication method: either **Windows** or **SQL Server**.
   a. If you select SQL Server Authentication, enter a **Login ID** and **Password**.
6. The option to **Enable interleaving for database transactions** is selected by default.

   This option 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.

   > **NOTE:**
   > If only one disk is present, deselect the option.

7. Click **Test Connection** to verify the server details.
8. In the **Job Owner Username** box, enter a SQL Server username 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 validate for it.
>
> For more information on the maintenance jobs, see Upgrade the ControlPoint databases to 5.6.1, on page 88.

9. Click **Next**.

   The ControlPoint Database Configuration page opens.

   > **NOTE:**
   > If you selected the option to interleave database transaction interleaving in step 6, the page indicates the paths participating in the interleaving.

   - **Data File.**
   - **Index File.**
   - **Text File.**
   - **Data Analysis Data.**
   - **Data Analysis Text.**
   - **Log file.**

   Click **Next.**

   The ControlPoint Audit Database Configuration page opens.

10. For each setting for the ControlPoint Audit database, specify the path, or click the browse button to define the path.

    > **NOTE:**
    > If you selected the option to interleave database transaction interleaving in step 6, the page indicates the paths participating in the interleaving.

    - **Data File.**
    - **Index File.**
    - **Text File.**
    - **Log file.**

      Click **Next.**

      The ControlPoint Tracking Database Configuration page opens.

11. For each setting for the ControlPoint Tracking database, specify the path, or click the browse button to define the path.

    > **NOTE:**
    > If you selected the option to interleave database transaction interleaving in step 6, the page

> indicates the paths participating in the interleaving.

- **Data File.**
- **Index File.**
- **Text File.**
- **Log file.**

  Click **Next.**

  The ControlPointMetaStore Database Configuration page opens.

12. For each setting for the ControlPoint MetaStore database, specify the path, or click the browse button to define the path.

> **NOTE:**
> If you selected the option to interleave database transaction interleaving in step 6, the page indicates the paths participating in the interleaving.

- **Data File.**
- **Index File**
- **Text File**
- **Metadata Data**
- **Metadata Index**
- **Metadata Text**
- **Metastore Data**
- **Metastore Index**
- **Metastore Text**
- **Metastore LDC Data**
- **Metastore LDC Index**
- **Metastore LDC Text**
- **Metastore Pro Data**
- **Metastore Pro Index**
- **Metastore Pro Text**
- **MS LDC Cache Data**
- **MS LDC Cache Index**
- **MS LDC Cache Text**
- **Log file.**

  Click **Next.**

The ControlPointMetaStoreTags Database Configuration page opens.

13. For each setting for the ControlPoint MetaStoreTags database, specify the path, or click the browse button to define the path.

    > **NOTE:**
    > If you selected the option to interleave database transaction interleaving in step 6, the page indicates the paths participating in the interleaving.

    - **Data File.**
    - **Index File.**
    - **Text File.**
    - **Log file.**

    Click **Next.**

    The Backup Confirmation page opens.

14. To confirm that you have backed up the databases before upgrade, click **I have backed up the databases**.

15. Click **Next**.

    The ControlPoint Audit Reports page opens.

16. To upload audit reports to SQL Server Reporting Services (SSRS), select **Upload Reports** and click **Next**.

    > **NOTE:**
    > This step requires that a data source in SQL Server Reporting Services was configured as a prerequisite. For more information, see Configure the ControlPoint data source, on page 22.

    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** box.

    b. In the Report Manager Server Settings area, enter the following information:

       i. **Report Manager URL.**

       ii. **Report Manager Virtual Directory.**

       > **NOTE:**
       > These settings are defined in the SQL Server Reporting Services Configuration Manager on the **Report Manager URL** tab. See step 5 of Configure the ControlPoint data source, on page 22.

       iii. **Report Webservice Virtual Directory.**

       > **NOTE:**
       > This is the virtual directory defined in the SQL Server Reporting Services Configuration Manager on the **Web Service URL** tab. See step 4 of Configure

> the ControlPoint data source, on page 22.

17. Click **Next**.

18. 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 upgrade. If the scripts encounter problems during execution, the database installation program displays a dialog box prompting you to **Retry** or **Abort**.
    >
    > If you choose to abort the execution, 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 **temp_db** 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.

19. Review the installation log.

20. Click the hyperlink to copy the connection string to your clipboard. The ControlPointMetaStore service requires this connection string to access the ControlPointMetaStore database.

    Save this connection string for configuring your ControlPoint IDOL package in step 14 of Configure deployment packages, on page 33.

21. Click **Finish**.

    The installation wizard closes.

Post upgrade step

After the database upgrade completes, do the following:

1. Verify the new SQL maintenance jobs.
2. If the **ControlPointMetaStore** and **tempDB** databases were not installed on dedicated hard drives, ensure that each is moved to their own dedicated hard drive. For example, **ControlPointMetaStore** is located on its own dedicated drive and **tempDB** is located on its own dedicated drive.

Verify the new SQL maintenance jobs

To verify the jobs

- In SQL Server Management Studio, navigate to **SQL Server Agent > Jobs** to verify the existence of ControlPoint database maintenance jobs.

  For each ControlPoint database, two maintenance jobs are created:

  - **<databaseName>_db_maint_3.0.** The database maintenance job that by default, runs automatically at 10 pm every night.
  - **<databaseName>_db_maint_all.** The database maintenance job that you can run manually as needed.

  where

  <databaseName> is the name of the ControlPoint database.

  For example:

  ControlPoint_db_maint_3.0 and ControlPoint_db_maint_all

  > **NOTE:**
  > The **_all** version of the maintenance script does not have a schedule defined, as it is intended to be run manually.

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://msdn.microsoft.com/en-us/library/ms345483(v=sql.120).aspx.

Example

This example describes the process of moving 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:**
   > **TempDB** 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**.

ControlPoint databases and performance considerations

The upgrade of the databases to ControlPoint 5.6.1 prepares your environment for file groups and database partitioning.

At this point, you should determine whether you want to take full advantage of the file groups and database partitioning. These improvements are especially important for the performance and scalability of large-scale ControlPoint environments.

> **NOTE:**
> Supported environments include those editions of SQL Server that support database partitioning and file groups (Enterprise editions of 2012, 2014, or 2016, and the Standard edition of SQL Server 2016 SP1).
>
> For more information on database partitioning, see your SQL Server documentation and the Software Requirements, on page 15.

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

To install the software

1. From the `\ControlPoint x64` directory, run `Setup.exe`as the Administrator, and then follow the instructions in the installer.
2. While the old IDOL software is still running, run the **Configuration Manager** and deploy ControlPoint.

   a. For environments where IDOL is enabled with HTTPS, in the `ControlPointConfiguration.exe.config` file, set the `<appSettings>` "`SecurePorts`" value to be `true`.

      For example:

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

   b. Save the `ControlPointConfiguration.exe.config` file.

   c. Run **Configuration Manager**.

   > **NOTE:**
   > If ControlPoint is running on HTTPS before the upgrade and you want to enable it again, follow the instructions in Enable HTTPS .

   The ControlPoint software installs.

Verify the databases in IDOL

Before upgrading the IDOL software, take note of the databases present, so that you can verify them after the upgrade.

To verify the databases

Issue a GETSTATUS command:

For HTTP: `http://`*`IDOLServerName`*`:9000/a=getstatus`

For HTTPS: `https://`*`IDOLServername`*`:9000/a=getstatus`

The IDOL databases are displayed.

Upgrade IDOL data and software

To upgrade the IDOL data and software

1. Back up any IDOL and connector configuration files that you modified manually or through the use of the ControlPoint software. This ensures that you can reapply the changes after the upgrade completes.

   Ensure that you copy all `*.cfg` files from your installation directory to another location. All IDOL files are already modified when new databases are added.

   > **NOTE:**
   > Any configuration file marked by a modification date later than the date of deployment indicates that it was modified manually or through the use of ControlPoint software.

2. Run the **ControlPoint IDOL Upgrade** program, which is available at the following location:

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

   Follow the instructions in the wizard.

   - For environments where IDOL is enabled with HTTPS, in the `ControlPointIDOL Upgrade.exe.config` file, set the `<appSettings>` "`SecurePorts`" value to be `true`.

     For example:

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

     The file is located in the `\Install\Program Files\Micro Focus\ControlPoint\Engine\Scheduler` directory.

   - For environments with multi-layer IDOL DIH/DAH, in the `ControlPointIDOL Upgrade.exe.config` file, edit the settings to reference the machine and correct port for the top-layer IDOL proxy.

3. Depending on the version of ControlPoint you are upgrading from, the upgrade may 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 upgrade process, you can save progress so you can resume the process 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.

Upgrade the IDOL software manually

When prompted, you must update the IDOL software manually.

If you are upgrading from ControlPoint 4.5 or earlier, this step also deploys an additional service, ControlPoint MetaStore.

To manually update the IDOL software

1. Ensure that you have a backup of all IDOL content and categories.

   If you are creating a new installation directory, then you must back up the `category` directory from the previously installed version of ControlPoint (`category, cluster, imex` and `taxonomy` directories).

   The files are located in the following locations:

   - **ControlPoint 4.5 or earlier** — `Program Files\Micro Focus\MF ControlPoint\Indexer\IDOL\category`
   - **ControlPoint 5.0 and later** — `Program Files\Micro Focus\ControlPoint\Indexer\IDOL\category`

2. Stop the IDOL services by running the `_stop_services.bat` batch file generated by the IDOL deploy tool.

   This batch file is available at `C:\temp\ControlPoint\`*`host_servername`*.

   You may need to run it from the command line with administrator permissions.

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

3. Uninstall existing services using `_uninstall_services.bat`.

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

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

   > **NOTE:**
   > Use the same Host Installation Directory as your current deployment. It ensures that your IDOL data migrates correctly.

   - For versions of ControlPoint earlier than 4.2, the Host Installation Directory is `C:\Program Files\Autonomy`.
   - For ControlPoint 4.3 to 4.6, the Host Installation Directory is `C:\Program Files\Micro Focus\ControlPoint`.

- For ControlPoint 5.1, the Host Installation Directory is `C:\Program Files\Micro Focus\ControlPoint`.

The deployment is prepared.

5. Do the following:

   a. Manually replace the `INSTALLATION_PATH\ControlPoint\Commons\jre` folder with a copy of the `temp\ControlPoint\`*host_XXX*`\Commons\jre` folder.

   b. Run the `_deploy_services.bat` file and choose to overwrite all files.

> **NOTE:**
> ControlPoint 5.6.1 installation requires Microsoft Visual C++ 2013 Runtime. This is provided with your ControlPoint software in the `vcredist` directory of your IDOL deployment package.
>
> Install it before running the `_install_services.bat` file, if you have not already done so.

6. Run the `_install_services.bat` batch file using the **As Administrator** option.

   The new services are installed.

Update configuration files

Update Connector configuration files

Update the Connector and Connector framework configuration files so that they match the configurations used in the previous deployment.

1. Perform the following key changes to the new configuration files after deployment:

   - **Contents:** Do the following:

     - Copy over the `[Databases]` section, for example:

       ```
       [Databases]
       NUMDBS=4
       0=News
       1=Archive
       2=FS
       3=SPS
       ```

     - Copy over `[Repositories]` section at bottom.

> **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:** Copy over 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
  ```

- **Each connector:** Copy over every `Task` section.

  For example:

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

- **For some connector types (such as SharePoint)**, additionally copy over 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 5.6.1 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, the total number must be increased as shown below:
`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.
>
> In version 4.2, the default task name changed from **MyTask** to **MyTask0**, so if you use default tasks and upgrade from a version earlier than 4.2, you must change the new connector configuration files accordingly.

- **Each connector framework**. Copy over each Eduction settings section.

  For example:

  ```
  [FSEductionSettings]
  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=eduction\number_ss_us.ecr
  ```

2. **Connector Framework**. Copy over 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 configuration files**. 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, you must edit the appropriate SharePoint connector configuration files as follows:

   a. Add the following section anywhere in the file:

   ```
   [Eduction]
   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 so that they match the configurations used in the previous deployment.

```
C:\Program Files\Micro Focus\ControlPoint\InsertConfig\
```

> **NOTE:**
> Ensure that the `InsertConfigEnabled` parameter in the `<AppSettings>` in `ControlPointTimer.config` is set to **true** to enable insert configurations.
>
> ```
> C:\Program Files\Micro
> Focus\ControlPoint\Engine\Scheduler\ControlPointTimer.exe.config.
> ```

Update Insert Configurations for Micro Focus Content Manager connectors

In ControlPoint 5.6.1, the Content Manager connector uses the `TRIM` folder in the insert configuration.

> **NOTE:**
> TRIM was the name of the Content Manager connector in releases before 5.4.

You may need to edit the TRIM insert configuration file with the custom insert configuration from your existing environment.

Update the configuration after upgrading to 5.6.1 by one of the following methods:

- On the Insert Configurations page, you must use TRIM for the Content Manager connector.
- You must use the TRIM custom field names, for example, `AU_PHASE_TrimOriginName` rather than `AU_PHASE_HPRMOriginName`.
- You can also re-add the custom fields in the Insert Configurations page.

  For more information on Insert Configurations, see the *ControlPoint Administration Guide* or the ControlPoint Console help system.

Integrate IDOL proxy updates

Perform the following key changes to the various upgrade scenarios for IDOL proxy updates in 5.6.1:

- **Database** upgrade - The 5.6.1 DB installer should take care of the database upgrade for IDOL proxy updates.
- **ControlPoint** upgrade - For all of the major upgrades such as uninstall, reinstall and for redeployment, you must follow the regular ControlPoint upgrade process. It is also recommended that before the upgrade process, you should backup all the configuration files in ControlPoint.
- **IDOL** upgrade - This can be achieved only by manually updating all the installed Connector and CFS configuration files as shown below:

```
Connector cfg:

Update [ViewServer] port with VIEW server port.

CFS cfg:

Update [MyIdolIndexer] port with DIH server port.

Update [Categorizer] port with CATEGORY server port.
```

Update Content Manager Connector configuration files

Beginning in the 5.4 release, the Content Manager connector replaced the Records Manager and TRIM connectors. Extra configuration in the connector configuration file is required for existing Records Manager or TRIM connectors to work with the Content Manager connector.

To configure the connector

1. Copy all `SynchronizeGroups` settings from the `FetchTasks` section of existing Records Manager and TRIM configuration files to the `FetchTasks` section of the configuration file for Content Manager, incrementing the settings as needed.

   Example

   In this example, the upgraded environment includes one Records Manager connector and one TRIM connector with the following settings.

   Original Records Manager settings

   ```
   SynchronizeGroupsNumber=4
   SynchronizeGroups0=Groups_TaskCm_1
   SynchronizeGroups1=Groups_TaskCm_2
   SynchronizeGroups2=Groups_TaskCm_3
   SynchronizeGroups3=Groups_TaskCm_4
   ```

   Original TRIM settings

   ```
   SynchronizeGroupsNumber=4
   SynchronizeGroups0=Groups_Tasktrim_1
   SynchronizeGroups1=Groups_Tasktrim_2
   SynchronizeGroups2=Groups_Tasktrim_3
   SynchronizeGroups3=Groups_Tasktrim_4
   ```

Copy the settings from Records Manager and TRIM `[FetchTasks]` sections to the **Content Manager** `[FetchTasks]` setting, and increment the `SynchronizeGroups` numbers as needed.

Set `SynchronizeGroupsNumber` to the total number of groups. In this example, set it to 8.

Resulting configuration settings

```
[FetchTasks]
SynchronizeGroupsNumber=8
SynchronizeGroups0=Groups_TaskCm_1
SynchronizeGroups1=Groups_TaskCm_2
SynchronizeGroups2=Groups_TaskCm_3
SynchronizeGroups3=Groups_TaskCm_4
SynchronizeGroups4=Groups_Tasktrim_1
SynchronizeGroups5=Groups_Tasktrim_2
SynchronizeGroups6=Groups_Tasktrim_3
SynchronizeGroups7=Groups_Tasktrim_4
```

2. **For Records Manager connectors**

> **NOTE:**
> This configuration is required because of differences in formatting of the older configurations in relation to version 5.6.1.

a. At the end of the file, edit all `IngestAction` values from `8` to `6`:

```
IngestActions=META:CPREPOSITORYTYPEID=8,META:AUTN_NO_FILTER=true
```

to

```
IngestActions=META:CPREPOSITORYTYPEID=6,META:AUTN_NO_FILTER=true
```

For example, edit the following values:

```
[Groups_TaskCm_54_repometa]
EnableGroupServerSecurity=True
SecurityType=TrimExt
AddSourceToMetadata=True
IngestActions=META:CPREPOSITORYTYPEID=8,META:AUTN_NO_FILTER=true
WorkgroupServer=myServerCm
WorkgroupServerPort=1137
DatabaseId=45
ScheduleStartTime=now
ScheduleCycles=1
ScheduleRepeatSecs=3600
IndexDatabase=CM_54_repometa
```

```
[TaskCm_54_repometa]
EnableGroupServerSecurity=True
SecurityType=TrimExt
AddSourceToMetadata=True
IngestActions=META:CPREPOSITORYTYPEID=8,META:AUTN_NO_FILTER=true
WorkgroupServer=myServerCm
WorkgroupServerPort=1137
```

```
DatabaseId=45
ScheduleStartTime=now
ScheduleCycles=1
ScheduleRepeatSecs=3600
IndexDatabase=Cm_54_repometa
```

to

```
[TaskCm_54_repometa]
EnableGroupServerSecurity=True
SecurityType=TrimExt
AddSourceToMetadata=True
IngestActions=META:CPREPOSITORYTYPEID=6,META:AUTN_NO_FILTER=true
WorkgroupServer=myServerCm
WorkgroupServerPort=1137
DatabaseId=45
ScheduleStartTime=now
ScheduleCycles=1
ScheduleRepeatSecs=3600
IndexDatabase=cm_54_repometa
```

```
[TaskCm_54_repometa]
EnableGroupServerSecurity=True
SecurityType=TrimExt
AddSourceToMetadata=True
IngestActions=META:CPREPOSITORYTYPEID=6,META:AUTN_NO_FILTER=true
WorkgroupServer=myServerCm
WorkgroupServerPort=1137
DatabaseId=45
ScheduleStartTime=now
ScheduleCycles=1
ScheduleRepeatSecs=3600
IndexDatabase=Cm_54_repometa
```

3. **For Records Manager and TRIM connectors prior to 5.x only.**

   Copy all `SynchronizeGroups` settings from the `FetchTasks` section of existing Records Manager and TRIM configuration files to the `FetchTasks` section of the configuration file for Content Manager, incrementing the settings as needed.

   ### Example

   In this example, the upgraded environment includes one Records Manager connector and one TRIM connector with the following settings.

   Original Records Manager settings

   ```
   SynchronizeGroupsNumber=4
   ```

   ```
   SynchronizeGroups0=Groups_TaskCM
   0=TaskCM
   SynchronizeGroups1=Groups_TaskCM_1
   1=TaskCM_1
   SynchronizeGroups2=Groups_TaskCM_2
   ```

```
2=TaskCM_43_2
SynchronizeGroups3=Groups_TaskCM_3
3=TaskCm_3
```

Original TRIM settings

```
SynchronizeGroupsNumber=4
SynchronizeGroups0=Groups_TaskTRIM
0=TaskTRIM
SynchronizeGroups1=Groups_Tasktrim_2
1=Tasktrim_2
SynchronizeGroups2=Groups_Tasktrim_3
2=Tasktrim_3
SynchronizeGroups3=Groups_Tasktrim_4
3=Tasktrim_4
```

Copy the settings from Records Manager and TRIM `[FetchTasks]` sections to the **Content Manager** `[FetchTasks]` setting, and increment the `SynchronizeGroups` numbers as needed.

Set `SynchronizeGroupsNumber` to the total number of groups. In this example, set it to 8.

Resulting configuration settings

```
[FetchTasks]
SynchronizeGroupsNumber=8
SynchronizeGroups0=Groups_TaskCM
0=TaskCM
SynchronizeGroups1=Groups_TaskCm_1
1=TaskCm_1
SynchronizeGroups2=Groups_TaskCm_2
2=TaskCm_43_2
SynchronizeGroups3=Groups_TaskCm_3
3=TaskCm_3
SynchronizeGroups4=Groups_TaskTRIM
4=TaskTRIM
SynchronizeGroups5=Groups_Tasktrim_2
5=Tasktrim_2
SynchronizeGroups6=Groups_Tasktrim_3
6=Tasktrim_3
SynchronizeGroups7=Groups_Tasktrim_4
7=Tasktrim_4
```

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 5.6.1 in a different directory than your previous installation directory, copy all `connector_repositoryname_datastore.db` files to the new installation directory.

3. When IDOL successfully starts, 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.

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.

   If you are upgrading from ControlPoint 4.5 or earlier, then there will be no MetaStore databases present at this point.

5. Return to the upgrade program and continue to follow the instructions.

   The program prompts you to start your connectors when the process completes.

6. 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.

7. Enable scheduled tasks.

8. To view previously updated repositories in the ControlPoint Dashboard, clear your browser cache, restart the browser and navigate to the repositories.

   For specific details on clearing the cache for your browser, see your browser's documentation.

9. If you are upgrading Records Manager or TRIM connectors from previous versions of ControlPoint to 5.6.1, edit the target locations to use the Content Manager connector and origin name.

The **Connector Group** and **Origin Name** fields are located on the Edit Target Location page.

For more information on editing target locations, see the *ControlPoint Administration Guide* or the Console Help system.

10. If you are upgrading Records Manager or TRIM connectors from previous versions of ControlPoint to use 5.6.1 and the Content Manager connector:

    - Edit the associated policies' **Target locations** field to the new connector. This field may be blank due to the change in connectors. The Target Location field is located on the Policy Phase page.

      For more information on editing policies, see the *ControlPoint Administration Guide* or the Console Help system.

11. If you are upgrading from Micro Focus Storage Optimizer to ControlPoint, you must rescan your existing scanned repositories and re-analyse the existing analysed repository to check the analysis summary.

Rescan repositories with custom properties after the upgrade

> **IMPORTANT:**
> The following procedure applies only to environments in the following states:
>
> - Environments upgraded to ControlPoint 5.5 but 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 in 5.6.1. For more information, see ControlPoint databases and performance considerations, on page 96 and the *ControlPoint Database Conversion Guide.*

If your ControlPoint environment has been configured with custom properties in repositories, additional steps are required after upgrading to 5.6.1.

For more reference material on configuring MetaStore for metadata ingestion, see Configure ControlPoint MetaStore for metadata ingestion, on page 128 or the *ControlPoint Administration Guide* and ControlPoint Console Help system.

To deal with 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 Edge Filesystem connector

> **NOTE:**
> Skip this step if you do not have ControlPoint Edge Filesystem connectors in your environment.

To upgrade the Edge Filesystem connector

1. Back up the Edge Filesystem Connector `.config` and `.db` files.

2. Uninstall the Edge Filesystem Connector and then the archive service:

   - **For Windows:** Uninstall the connector from the Windows **Add/Remove** Programs option.

   - **For Linux:** Change the directory to the `SORHELInstall` directory and run the following command:

     ```
     sudo sh sosetup.sh remove
     ```

3. Restart the system.

4. Install the new version of the Edge Filesystem Connector and archive service, then restart the system.

   For more information, see Install the Edge Filesystem connector, on page 56.

5. After the system restarts, stop the Edge Filesystem Connector and copy the `task` section and any other manual modifications from the backed up `.config` file to the new version of the `config` file. Also copy the `.db` files into the connector directory.

6. Start the Edge Filesystem Connector.

Edge Filesystem Connector configuration file

The Edge Filesystem Connector configuration file for Windows and Linux has a new config section "EnableSSL", which is disabled by default.

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

If IDOL on the ControlPoint server is already using HTTPS, the Edge Filesystem Connector should also use HTTPS in order to be listed on the connection list on the Repository page in the ControlPoint Dashboard.

All other HTTPS configurations to run the Edge Filesystem Connector on HTTPS are similar to the configuration on a regular Filesystem connector.

Chapter 11: Troubleshooting

This section provides troubleshooting information on the following:

- Databases, below
- Connectors
  - Edge Filesystem Connectors
  - SharePoint Connectors
  - Content Manager connector, on page 119
- Proxy server interactions
- IDOL
  - Preview of items on remote connectors
  - HTTPS setup for IDOL
  - IDOL distributed mirror / non- mirror setup
- Policy execution
- Diagnostics logs
  - Policy Execution Logs
  - Data Analysis logs
  - Statistics Export utility trace logs

Databases

This section describes some items for your ControlPoint databases.

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

In the 5.6.1 release, several modifications have been made to the Compact stored procedure:

- Prevent more than one Compact job from running at a time.
- Always delete all repositories that are marked for deletion.
- Perform the cleanup of unused hashes on a limited number of repositories.

Two new settings have been introduced to the **ControlPointMetaStore.Metadata.Settings** table to control the Compact stored procedure. You can adjust the 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 feel the Compact stored procedure is stuck and not completing after one week, you can clear the IsRunning flag.

To clear the 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'
```

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 = "SSLV23",
    }
   ```

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 eduction 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 it is known in advance that eduction grammars will be specified that will likely generate a lot of metadata for each document then you should 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

Linux Edge Filesystem Connector in a distributed connector system does not belong to the same domain as ControlPoint

Problem

The Edge Filesystem Connector is installed on a Linux environment in a distributed connector system that does not belong to the same domain as ControlPoint.

Solution

1. Stop the Edge Filesystem Connector.
2. On the Distributed Connector system, edit the `hosts` file to add the Edge Filesystem Connector.
3. On the Distributed Connector system, ensure that ports 7210 and 7212 are enabled with the Edge Filesystem Connector machine, or turn off the firewall.
4. On the Edge Filesystem Connector system, ensure that ports 7210 and 7212 are enabled, or turn off the firewall.
5. Start the Edge Filesystem Connector.

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 connector

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: FETCHTASKS: 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

The workaround is to create a new policy for the insert action and to create 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* or Console help system.

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.

IDOL

This section provides troubleshooting information for the IDOL components.

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 can not 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 `\Program Files\Micro Focus\ControlPoint\Engine\Scheduler\ControlPointTimer.exe.config` in the production environment.

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, on the previous page
Erroneous GlobalSettings table settings.	For more information on global settings, see the *ControlPoint Best Practice Guide*.

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.

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 `\Program Files\Micro Focus\ControlPoint\Engine\Scheduler\ControlPointTimer.exe.config` in the production environment.

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">`

     > **NOTE:** 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 x64\ControlPoint 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.

Chapter 12: Configure ControlPoint MetaStore for metadata ingestion

This section provides an overview of the steps necessary for configuring ControlPoint MetaStore 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=”BFS”, NUMBER=10, STREET=”Queens”}. 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.
ExtractPath	The value of this field is typically null, except when a value is to

Field	Description
	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: • “MVF” if the table can capture multiple values for the same document. For example, more than one row can exist for a given document. • “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.

Field	Description

TargetMVPSuffix	Supports the extraction of a suffix from the source field name to further populate a column in the target table.
	For example, assuming data exists in the source document like:
	CPPATH1=\\c\
	CPPATH2=\\c\test\
	CPPATH3=\\c\test\folder\
	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”.

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
@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_STRIN`G 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 13: ControlPoint Multi-domain configuration

This section describes the procedure to set up and use the multi-domain feature.

- Prerequisites
- Configure
- Test

Prerequisites

This section lists 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 user s 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 able to query LDAP/AD to get all domain user information.
5. Ensure all machines with CointolPoint 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

To set up multi-domain support.

1. In the ControlPoint user interface, click **Administration** -> **Additional Domain Registration**, and the 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

[Categorizer]

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

After set up, Micro Focus strongly recommends you perform the following tests:

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 post-installation tasks

After the installation is complete, you must update the following ControlPoint configuration files with the settings **in bold**:

> **NOTE:**
> Ensure to restart the ControlPoint services after the configuration files are updated.

- ControlPoint Timer configuration
- Dashboard configuration
- ControlPoint IDOL configuration
- ControlPoint OGS configuration
- Filesystem Connector configuration
- SharePoint Remote Connector configuration
- Documentum Connector configuration

ControlPointTimer.exe.Config

```
<idolServersConfigurationSection default="Default System">

<idolServers>

<idolServer name="myIdolServer" host="localhost" port="9000" indexPort="9001"

connectorHost="localhost" connectorPort="7000" defaultLanguage="ENGLISH"

defaultEncoding="UTF8" useSecurity="false" connectionLimit="100"

OGSHost="myOGSServer.myDomain.com" OGSPort="4057"/>

</idolServers>

</idolServersConfigurationSection>
```

Dashboard.config

```
<idolServersConfigurationSection default="Default System">

<idolServers>

<idolServer name="Default System" host="localhost" port="9000" indexPort="9001"

connectorHost="localhost" connectorPort="7000" dahHost="localhost" dahPort="9060"

defaultLanguage="ENGLISH" defaultEncoding="UTF8" useSecurity="true"
deferLogin="true"

connectionLimit="100" metaStoreHost="localhost" metaStorePort="4500"
```

```
sqlConnectionString="Persist Security Info=False;Application Name=ControlPoint
Dashboard;Server=.;Database=ControlPointMetaStore;Integrated Security=true;User
ID=;Password="

OGSHost="myOGSServer.myDomain.com" OGSPort="4057"/>

</idolServers>

</idolServersConfigurationSection>
```

> **NOTE:**
> The configuration files `ControlPointTimer.exe.Config` and `Dashboard.config` are case-sensitive.

ControlPoint IDOL cfg

```
[UserSecurity]

9=NT

[NT]

GroupServerHost= OGSHost

GroupServerPort=OGSPort

GroupServerRepository=LDAP

[LDAP]

LDAPServer=LDAPServerHost

LDAPPort=389

[SharePoint]

GroupServerHost= OGSHost

GroupServerPort=OGSPort

GroupServerRepository=LDAP

[Documentum]

DocumentSecurity=TRUE

GroupServerHost=OGS _Host

GroupServerPort=OGS_Port

SecurityFieldCSVs=username

DocumentSecurityType=Documentum_V4

CaseSensitiveUserNames=FALSE

CaseSensitiveGroupNames=FALSE

GroupServerPrefixDomain=false

GroupServerOpApplyTo0=USER
```

```
GroupServerOp0=Prepend

GroupServerOpParam0=YourDomainName\
```

ControlPoint OGS cfg

```
[Repositories]

GroupServerDefaultRepositories=HPRecordsManager,TRIM,SharePoint2007,SharePoint2010,
SharepointRemote,WorkSite,SharePoint2013,Documentum,LDAP

Number=9

0=HPRecordsManager

1=TRIM

2=Sharepoint2007

3=Sharepoint2010

4=SharepointRemote

5=WorkSite

6=Sharepoint2013

7=Documentum

8=LDAP

[LDAP]

GroupServerLibrary=ogs_ldap.dll

LDAPServer=LDAPServerHost

LDAPPort=389

LDAPBase=DC=

LDAPType=MAD

LDAPBindMethod=NEGOTIATE

GroupServerAllUserGroups=NT AUTHORITY\AUTHENTICATED USERS

GroupServerCycles=-1

UseDomainPrefix=True

DomainPrefix=DOMAINPREFIX

[Documentum]

GroupServerLibrary=ogs_java

JavaGroupServerClass=com.autonomy.groupserver.documentum.DocumentumGroupServer

Docbase=MyDocBase

Username=UserName
```

```
Password=********
//Note, docBase and userName are casesensitive,
GroupServerCycles=-1
GroupServerQueryOp0=StartAfter
GroupServerQueryOpApplyTo0=USER
GroupServerQueryOpParam0=0;\
GroupServerShowAlternativeNames=true
UserNameFields=user_login_name
```

Filesystem Connector cfg

```
[Ingestion]
IngestActions=META:ENFORCESECURITY=True,META:CPREPOSITORYTYPEID=3,META:SECURITYTYPE=NT
[FetchTasks]
MappedSecurity=True
GroupServerHost=OGSHost
GroupServerPort=OGSPort
GroupServerRepository=NT
```

SharePoint Remote Connector cfg

```
[Ingestion]
IngestActions=META:ENFORCESECURITY=True,META:CPREPOSITORYTYPEID=9,META:SECURITYTYPE=SharePointSecurity
[FetchTasks]
GroupServerHost=OGSHost
GroupServerPort=OGSPort
GroupServerRepository=sharepointRemote
EncryptACLEntries=False
MappedSecurity=TRUE
```

Documentum Connector cfg

```
[Ingestion]
IngestActions=META:ENFORCESECURITY=True,META:CPREPOSITORYTYPEID=17,META:SECURITYTYPE=Documentum
```

Also perform the following:

Copy the `Documentum dfc` libraries to `Program Files\Micro Focus\ControlPoint\Commons\dfc` folder.

> **NOTE:**
> The libraries are not redistributable. For any help related to library access, you may always get in touch with the Documentum Support team.

Appendix B: ControlPoint post-upgrade tasks

After the upgrade completion, you must update the following ControlPoint configuration files with the settings **in bold**:

> **NOTE:**
> Ensure to restart the ControlPoint services after the configuration files are updated.

- ControlPoint Timer configuration
- Dashboard configuration
- ControlPoint IDOL configuration
- ControlPointOGS configuration
- Content configuration
- Filesystem Connector configuration
- Filesystem Connector framework configuration
- SharePoint remote Connector configuration
- SharePoint remote Connector framework configuration
- Documentum Connector configuration
- Documentum Connector framework configuration
- Exchange Connector framework configuration
- Content Manager Connector framework configuration
- Notes Connector Framework cfg

ControlPointTimer.exe.Config

```
<idolServersConfigurationSection default="Default System">

<idolServers>

<idolServer name="myIdolServer" host="localhost" port="9000" indexPort="9001"

connectorHost="localhost" connectorPort="7000" defaultLanguage="ENGLISH"

defaultEncoding="UTF8" useSecurity="false" connectionLimit="100"

OGSHost="myOGSServer.myDomain.com" OGSPort="4057"/>

</idolServers>

</idolServersConfigurationSection>
```

Dashboard cfg

```
<idolServersConfigurationSection default="Default System">
```

```
<idolServers>

<idolServer name="Default System" host="localhost" port="9000" indexPort="9001"

connectorHost="localhost" connectorPort="7000" dahHost="localhost" dahPort="9060"

defaultLanguage="ENGLISH" defaultEncoding="UTF8" useSecurity="true"
deferLogin="true"

connectionLimit="100" metaStoreHost="localhost" metaStorePort="4500"

sqlConnectionString="Persist Security Info=False;Application Name=ControlPoint
Dashboard;Server=.;Database=ControlPointMetaStore;Integrated Security=true;User
ID=;Password="

OGSHost="myOGSServer.myDomain.com" OGSPort="4057"/>

</idolServers>

</idolServersConfigurationSection>
```

ControlPoint IDOL cfg

```
[UserSecurity]

9=NT

[NT]

GroupServerHost= OGSHost

GroupServerPort=OGSPort

GroupServerRepository=LDAP

[LDAP]

LDAPServer=LDAPServerHost

LDAPPort=389

[SharePoint]

GroupServerHost= OGSHost

GroupServerPort=OGSPort

GroupServerRepository=LDAP

[Documentum]

DocumentSecurity=TRUE

GroupServerHost=OGS _Host

GroupServerPort=OGS_Port

SecurityFieldCSVs=username

DocumentSecurityType=Documentum_V4

CaseSensitiveUserNames=FALSE
```

```
CaseSensitiveGroupNames=FALSE

GroupServerPrefixDomain=false

GroupServerOpApplyTo0=USER

GroupServerOp0=Prepend

GroupServerOpParam0=YourDomainName\
```

ControlPoint OGS cfg

```
[Repositories]

JavaClassPath0=.

JavaClassPath1=./*.jar

JavaClassPath2=./lib/

JavaClassPath3=./lib/*.jar

JavaClassPath4=Path to \ControlPoint\Commons\dfc/*.jar

JavaMaxMemoryMB=256

JVMLibraryPath=Path to \ControlPoint\Commons\jre\bin\server

GroupServerDefaultRepositories=HPRecordsManager,TRIM,SharePoint2007,SharePoint2010,
SharepointRemote,WorkSite,SharePoint2013,Documentum,LDAP

Number=9

0=HPRecordsManager

1=TRIM

2=Sharepoint2007

3=Sharepoint2010

4=SharepointRemote

5=WorkSite

6=Sharepoint2013

7=Documentum

8=LDAP

[LDAP]

GroupServerLibrary=ogs_ldap.dll

LDAPServer=LDAPServerHost

LDAPPort=389

LDAPBase=DC=

LDAPType=MAD
```

```
LDAPBindMethod=NEGOTIATE
GroupServerAllUserGroups=NT AUTHORITY\AUTHENTICATED USERS
GroupServerCycles=-1
UseDomainPrefix=True
DomainPrefix=DOMAINPREFIX
[Documentum]
GroupServerLibrary=ogs_java
JavaGroupServerClass=com.autonomy.groupserver.documentum.DocumentumGroupServer
Docbase=MyDocBase
Username=UserName
Password=********
GroupServerCycles=-1
GroupServerQueryOp0=StartAfter
GroupServerQueryOpApplyTo0=USER
GroupServerQueryOpParam0=0;\
GroupServerShowAlternativeNames=true
UserNameFields=user_login_name
```

Content.cfg

```
[Server]
KillDuplicatesPreserveFields=
[LanguageTypes]
AugmentSeparators=.
```

FileSystem Connector cfg

```
[Ingestion]
IngestActions=META:ENFORCESECURITY=True,META:CPREPOSITORYTYPEID=3,META:SECURITYTYPE=NT
[FetchTasks]
MappedSecurity=True
GroupServerHost=OGSHost
GroupServerPort=OGSPort
GroupServerRepository=NT
```

Filesystem Connector Framework cfg

```
[ImportTasks]
Pre0=lua:lua/SetIndexType.lua
Pre1=lua:lua/NoExtract.lua
Hash0=lua:lua/hash.lua
Post0=lua:lua/ExtractFilename.lua
Post1=Standardizer
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
[actions]
MaxQueueSize=100000
[Eduction]
DefaultMaxMatchesPerDoc=10000
```

SharePoint Remote Connector cfg

```
[Ingestion]
IngestActions=META:ENFORCESECURITY=True,META:CPREPOSITORYTYPEID=9,META:SECURITYTYPE=SharePointSecurity
[FetchTasks]
Number=1
GroupServerHost=OGSHost
GroupServerPort=OGSPort
GroupServerRepository=sharepointRemote
SynchronizeGroupsNumber=1
SynchronizeGroups0= Groups_TaskSPRemote
EncryptACLEntries=False
MappedSecurity=TRUE
```

SharePoint Remote Connector Framework cfg

```
[ImportTasks]
Pre0=lua:lua/SetIndexType.lua
Pre1=lua:lua/NoExtract.lua
Pre2=lua:lua/RepositoryTitleFixup.lua
Hash0=lua:lua/hash.lua
Post0=Standardizer
Post1=lua:lua/ExtractFilenameInheritTitle.lua
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
[actions]
MaxQueueSize=100000
[Eduction]
DefaultMaxMatchesPerDoc=10000
[IndexTasks]
Update0=lua:lua/securityupdate.lua
```

Documentum Connector cfg

```
[Ingestion]
IngesterType=CFS
IngestHost=YourHostName
IngestPort=7950
IngestBatchSize=100
IndexDatabase=DocumentumConnector
IngestActions=META:ENFORCESECURITY=True,META:CPREPOSITORYTYPEID=17,META:SECURITYTYPE=Documentum
[Default]
GroupServerHost=OGS _Host
GroupServerPort=OGS_Port
```

```
GroupServerRepository=Documentum
Username=Domain\UserName
Password=9v3t3t7awt/JjPA
RetentionExpirationTime=2038-JAN-01 00:00:00 GMT
[FetchTasks]
EncryptACLEntries=False
MappedSecurity=True
[TaskDocumentumFolder3]
IngestActions=META:CPREPOSITORYTYPEID=17,META:AUTN_NO_EXTRACT=true,META:AUTN_
CATEGORIZE=false,META:AUTN_EDUCTION=false,META:SECURITYTYPE=Documentum,
META:ENFORCESECURITY=true
EncryptACLEntries=False
docbase=MyTestRepo
folderCSVs=/MyTestRepo/FolderOne
ScheduleStartTime=now
ScheduleCycles=1
ScheduleRepeatSecs=3600
IndexDatabase=DocumentumFolder3
```

Documentum Connector Framework cfg

```
[ImportTasks]
Pre0=lua:lua/SetIndexType.lua
Pre1=lua:lua/NoExtract.lua
Hash0=lua:lua/hash.lua
Post0=lua:lua/ExtractFilename.lua
Post1=Standardizer
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
[actions]
MaxQueueSize=100000
```

```
[Eduction]

DefaultMaxMatchesPerDoc=10000

[IndexTasks]

Update0=lua:lua/securityupdate.lua
```

`Perform the following steps for Dcoumentum connector framework:`

1. Copy the `Documentum dfc` libraries to `Program Files\Micro Focus\ControlPoint\Commons\dfc` folder.

   > **NOTE:**
   > The libraries are not redistributable. For any help related to library access, you may always get in touch with the Documentum Support team.

2. Copy the `dfc.properties` and `dfc.keystore` files from the Documentum Server to the Documentum Connector folder. You can find the properties file in the `config directory` of your Documentum server installation.
3. Copy the `dfc.properties` and `dfc.keystore` files to `OGS` folder. You can find the properties file in the `config` directory of your Documentum server installation.

Exchange Connector Framework cfg

```
[ImportTasks]

Pre0=lua:lua/SetIndexType.lua

Pre1=lua:lua/NoExtract.lua

Hash0=lua:lua/hash.lua

Post0=Standardizer

Post1=lua:lua/Eduction.lua

Post2=lua:lua/MetadataProvider.lua

Post3=lua:lua/IndexingTarget.lua

Post4=lua:lua/CFSFixup.lua

Post5=lua:lua/Category.lua

[actions]

MaxQueueSize=100000

[Eduction]

DefaultMaxMatchesPerDoc=10000
```

Content Manager Connector Framework cfg

```
[ImportTasks]
```

```
Pre0=lua:lua/SetIndexType.lua
Pre1=lua:lua/NoExtract.lua
Hash0=lua:lua/hash.lua
Post0=Standardizer
Post1=lua:lua/ExtractFilenameInheritTitle.lua
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
[actions]
MaxQueueSize=100000
[Eduction]
DefaultMaxMatchesPerDoc=10000
```

Notes Connector Framework cfg

```
[ImportTasks]
Pre0=lua:lua/SetIndexType.lua
Pre1=lua:lua/NoExtract.lua
Hash0=lua:lua/hash.lua
Post0=Standardizer
Post1=lua:lua/Eduction.lua
Post2=lua:lua/MetadataProvider.lua
Post3=lua:lua/IndexingTarget.lua
Post4=lua:lua/CFSFixup.lua
Post5=lua:lua/Category.lua
[actions]
MaxQueueSize=100000
[Eduction]
DefaultMaxMatchesPerDoc=10000
```

Appendix C: 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 — see Synopsis, below for command line options and examples.

> **NOTE:**
> Command line enhancements are supported for ControlPoint 5.4 and later.
>
> For versions 5.3 or earlier, run the utility with the user interface.

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 `\<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

> **NOTE:**
> The following example applies to ControlPoint versions 5.4 and later. If you are running version 5.3 or earlier, this example does not apply.

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 and copies all of the system information and configuration file information and label it 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, the locations of the `Pre` and `Post` data files are as follows:

```
<systemroot>\Users\<user>\AppData\Local\Temp\PreLogFiles
```

```
<systemroot>\Users\<user>\AppData\Local\Temp\PostLogFiles
```

```
<systemroot>\Users\<user>\AppData\Local\Temp\PreSystemInfo.xml
```

```
<systemroot>\Users\<user>\AppData\Local\Temp\PostSystemInfo.xml
```

Appendix D: 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 Eduction 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 Eduction 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. You can find detailed documentation about the IDOL Media Server on the MySupport portal.

Before you begin

Ensure you have the following items:

- IDOL Media Server

  You can download this software from the Micro Focus Big Data Download Center.

- An IDOL license with media server enabled

If you need help obtaining any 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 on the same server as ControlPoint.

   After extraction, the application's root folder contains an `install.txt` file with installation instructions.

2. Configure the *`mediaServerInstallPath`*`/MediaServer.cfg` file:

   a. Open the `MediaServer.cfg` file in a text editor.

   b. Locate the `[Channels]` section and ensure its properties are set as follows:

   ```
   [Channels]
   # Make sure enough license channels are available to cover Process threads
   VisualChannels=1
   SurveillanceChannels=1
   AudioChannels=0
   VideoManagementChannels=0
   ```

   c. Locate the `[Server]` section and make note of the specified port number.

   You will use this value in subsequent steps.

   d. Save the file.

3. Configure the `ControlPoint Filesystem Connector framework.cfg` file:

   a. Open the `ControlPoint Filesystem Connector framework.cfg` file in a text editor.

   b. Locate the `[ImportTasks]` section and add the following tasks to it:

   ```
   PreX=lua:lua/OCR_Scan.lua
   PreX+1=lua:scripts/ImageAnalysis.lua
   ```

   Where ***X*** is the next number following the last existing task. For example, if a `Pre1` task exists, add the following:

   ```
   Pre2=lua:lua/OCR_Scan.lua
   Pre3=lua:scripts/ImageAnalysis.lua
   ```

   c. Add the following `[MediaServerSettings]` section:

   ```
   [MediaServerSettings]
   MediaServerHost=localhost:port
   MediaServerConfigurationName=ocrdoc.cfg
   MediaServerSharedPath=\\hostname\ocrSharedFolderPath
   MediaAnalysisTransform=./xslt/mediaserver_cfs_ocr.xsl
   ```

   where:

   - ***hostname\ ocrSharedFolderPath*** is an accessible path to an existing folder in which to store OCR documents.

     For example the following sets it to the `ocrdocuments` folder on a host named `jmc-srv2012-1`:

     ```
     MediaServerSharedPath=\\jmc-srv2012-1\ocrdocuments
     ```

   - ***port*** is the port number specified in the `[Server]` section of the `MediaServer.cfg` file.

     For example: `MediaServerHost=localhost:140000`

   d. Save the file.

4. Create the `OCR_Scan.lua` file.

   a. Create an `OCR_Scan.lua` file in the ControlPoint `FileSystem Connector Framework\lua` folder.

   b. Open the file in a text editor, and then copy and paste the following into it:

   ```
   -- Initialization lua
   dofile("lua/initialize.lua")
   require("constants")
   require("UtilityFunctions")

   -- Handler
   function handler(document)
      local extensions_for_ocr = { jpeg = 1, tif = 1, bmp = 1, png = 1, jpg =
   ```

```
1, pdf = 1};
   local filename = document:getFieldValue("DREREFERENCE");
   local extension, extension_found = filename:gsub("^.*%.(%w+)$", "%1", 1);

   if extension_found > 0 then
      if extensions_for_ocr[extension:lower()] ~= nil then
         document:addField("AUTN_NEEDS_IMAGE_SERVER_ANALYSIS", "");
      end
   end

   return true;
   end
```

c. Save the file.

5. Create the `ocrdoc.cfg` file:

   a. Create an `ocrdoc.cfg` file in the ControlPoint `Filesystem Connector Framework` folder.

   b. Open the file in a text editor, and then copy and paste the following into it:

```
// Example showing how to OCR document-style files

// ======================= Ingest ========================
[Ingest]
IngestEngine0 = Read

[Read]
// Ingest image and document file formats
Type = image

// ======================= Analysis =======================
[Analysis]
AnalysisEngine0 = OCR

[OCR]
Type = ocr

// Process printed document pages (rather than generic photos)
OCRMode = document

// Add any relevant languages to this list
Languages = en

// Filter out lower confidence words
WordRejectThreshold = 60

// ======================= Output =======================
[Output]
OutputEngine0 = response
```

```
[TextOut]
Type = xml
Input = OCR.Event
XMLOutputPath = output/%source.filename%.txt

// Extract just the text from output
XSLTemplate = xsl/toText.xsl

[response]
Type=response
```

c. Save the file.

6. Configure the `ImageAnalysis.lua` file, located in the ControlPoint `Filesystem Connector Framework/scripts` folder:

   a. Open the `ImageAnalysis.lua` file in a text editor.

   b. Replace the contents of the entire file with the following:

```
function handler(document)
   document:addField("Enter_Image_Analysis", "true");
   if mediaServerSupportsTypeInDocument(document) then
      -- Send the file to Media Server for analysis.  This will throw
      -- on failure resulting in an error being logged and the
      -- document being filtered by KeyView as normal (provided no
      -- later tasks disable filtering).
      document:addField("Enter_Analyze_Media", "true");
      document:addField("Shared folder",
         [[\\localhost\ocrSharedFolderPath]])
      document:addField("Shared OCR file",
         [[ocrSharedFilePath\ocrdoc.cfg]])
      -- geServerHost='localhost';
      -- geServerPort=port;
      -- geServerSharedPath=\\localhost\\ocrSharedFolderPath;
      analyze_media_in_document(document, {
         section = "MediaServerSettings",
         taskSections = dococrtask,
         server = {host="localhost",
            port = port,
            sharedPath = [[\\localhost\\ocrSharedFolderPath]] }} );
      document:addField("Enter_Analyze_Media_Complete", "true");
--
```

   where:

   - ***`ocrSharedFolderPath`*** is the path to the folder that stores OCR documents. For example: `ocrdocuments`.

     > **NOTE:**
     > This must be the same folder path you set for ***`ocrSharedFolderPath`*** in the framework.cfg file (Step 3c).

- ***ocrSharedFilePath*** is the path of the folder that contains the `ocrdoc.cfg` file you created in the previous step. For example:

  ```
  C:\newdisk\services\MediaServer_11.4.0\configurations
  ```

- ***port*** is the port number specified in the `[Server]` section of the `MediaServer.cfg` file. For example: `140000`.

c. Save the file.

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 Installation Guide (Micro Focus ControlPoint 5.6.1)

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!