

IBM FileNet P8 Platform
Version 5.2.0

*Installation Guide for installation on
Linux
with Oracle, IBM WebSphere
Application Server, and Windows Active
Directory*



IBM FileNet P8 Platform
Version 5.2.0

*Installation Guide for installation on
Linux
with Oracle, IBM WebSphere
Application Server, and Windows Active
Directory*



Note

Before using this information and the product it supports, read the information in “Notices” on page 205.

This edition applies to version 5.2.0 of IBM FileNet Content Manager (product number 5724-R81), version 5.2.0 of IBM FileNet Business Process Manager (product number 5724-R76), and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2001, 2013.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

ibm.com and related resources vii

How to send your comments vii

Contacting IBM. viii

Part 1. Installing a distributed FileNet P8 system 1

Installing FileNet P8 documentation. 3

Installing the local information center 3

 Installing the FileNet P8 information center interactively 4

 Installing the FileNet P8 information center silently 5

Starting and verifying the FileNet P8 information center. 6

Backing up and redeploying the FileNet P8 information center 6

Installing and configuring Content Platform Engine 9

Installing Content Platform Engine and IBM Case Foundation 10

 Installing Content Platform Engine 11

 Installing Content Platform Engine interactively 12

 Installing Content Platform Engine silently 13

 Installing Enterprise Manager 13

 Installing Content Platform Engine software updates. 14

 Installing IBM Case Foundation 15

 Installing IBM Case Foundation interactively 15

 Installing IBM Case Foundation silently 16

Configuring Content Platform Engine 17

 Granting directory permissions to the Configuration Manager user. 18

 Configuring Content Platform Engine instances 18

 Configuring Content Platform Engine instances by using the graphical user interface. 19

 Starting the Configuration Manager graphical user interface 20

 Changing the password save preference 20

 Creating a new configuration profile 21

 Configuring the global configuration database JDBC data source settings 22

 Configuring the initial object store data sources by using the graphical user interface 23

 Configuring the login modules (WebSphere and JBoss only) 24

 Configuring Content Platform Engine application server authentication (LDAP) settings. 25

 Configuring bootstrap and text extraction settings. 26

Configuring instances by using the command line 27

 Generating the configuration XML files for a Content Platform Engine instance 28

 Creating the data sources by using the command line 32

 Editing the configuration XML files for a Content Platform Engine instance 34

 Running the configuration XML files 37

 Checking the completion status of Content Platform Engine configuration tasks 41

Deploying Content Platform Engine instances 43

 Deploying instances by using the graphical user interface 44

 Deploying Content Platform Engine by using the Configuration Manager command line 45

 Generating the deployapplication.xml file 46

 Editing the deployment configuration files 47

 Running the deployapplication.xml file 48

 Checking the configuration status of the deployapplication task 49

Installing storage device source files 49

 Installing Tivoli Storage Manager client and adding native API library paths (WebSphere Application Server). 50

 Installing Tivoli Storage Manager client 50

 Copying the Tivoli Storage Manager API libraries to additional servers 50

 Creating a shared library definition for Tivoli Storage Manager native API library files. 51

 Installing or updating EMC Centera SDK library files 51

 Installing EMC Centera SDK library files 51

 Configuring EMC Centera SDK environment variables 52

Configuring file stores for high availability. 54

Completing Content Platform Engine post-deployment steps. 54

 Completing Content Platform Engine post-deployment steps (WebSphere) 54

Verifying the Content Platform Engine deployment 55

Creating the FileNet P8 domain 58

Creating a database connection. 58

Creating the initial object store 59

Creating a workflow system. 59

Connecting to a highly available Content Platform Engine 60

 Content Platform Engine in an application server cluster by using EJB transport 61

 Connecting by using Content Engine Web Service Transport (CEWS) 62

Verifying the Content Platform Engine system. 62

Installing and configuring IBM Content Search Services. 65

Installing IBM Content Search Services	66
Installing IBM Content Search Services interactively	67
Installing IBM Content Search Services silently	67
Starting or stopping IBM Content Search Services servers	68
Configuring IBM Content Search Services	69
Getting the IBM Content Search Services authentication token	69
Configuring Content Platform Engine for IBM Content Search Services	70
Configuring IBM Content Search Services servers on Content Platform Engine	71
Setting the indexing languages for an object store.	71
Creating an index area.	72
Disabling IBM Legacy Content Search Engine	73
Enabling text search on the object store	73
Configuring objects that can be indexed for content based retrieval.	74
Verifying the IBM Content Search Services installation	75
Configuring SSL for IBM Content Search Services	76
Encrypting data transmitted over the network	77
Performing SSL server authentication.	78
Deploying server certificates on IBM Content Search Services server	78
Deploying CA certificates on Content Platform Engine server	80
Validating certificates	81
Configuring the Content Platform Engine server to do host validation	82

Installing and configuring Application Engine 83

Installing Application Engine	84
Installing Application Engine interactively	85
Installing Application Engine silently	86
Verifying your Application Engine installation.	88
Installing Application Engine software updates	88
Installing the latest Content Platform Engine Client files on Application Engine servers	89
Installing the latest Content Platform Engine Client files on Application Engine servers interactively	89
Installing the latest Content Platform Engine Client files on Application Engine servers silently	90
Configuring Application Engine on the application server	91
Configuring Application Engine on WebSphere Application Server	92
Editing web.xml for container-managed authentication	93
Editing web.xml for SSO	95
Configuring Java Virtual Machine settings for JAAS login and memory	98
Configuring Lightweight Third Party Authentication (LTPA).	99
Configuring stand-alone Lightweight Directory Access Protocol (LDAP)	101

Configuring Lightweight Directory Access Protocol (LDAP) for federated repositories	102
Deploying Application Engine on the application server	103
Deploying Application Engine on WebSphere Application Server	104
Re-creating the WAR or EAR file	104
Deploying the application (WebSphere Application Server)	105
Setting Application Engine bootstrap preferences	107
Setting the bootstrap properties on first login	107
Verifying that a single index has been added for Application Name on the site preferences object store	110
Enabling user access to the workflow subscription wizard	110
Enhanced Timezone Detection	111
Updating Application Engine settings in a load balanced environment	111

Configuration and startup tasks 113

Configuring the workflow system connection point for Application Engine	113
Setting up Content Platform Engine and client transport SSL security	114
Enabling SSL for Content Platform Engine.	115
Enabling SSL between Enterprise Manager and the directory service	117
Enabling SSL between IBM Administration Console for Content Platform Engine and the directory service	117
Setting up Application Engine SSL security	117
Setting up full SSL support on a single Application Engine	118
Setting up SSL redirect on a single Application Engine server	118
Setting up SSL redirect on two Application Engine servers	119
Using Java Applets in an SSL Environment	120
Performing additional configuration tasks	120

Optional installation tasks 123

Installing and configuring IBM FileNet P8 publishing components	123
Installing FileNet Deployment Manager	123
Installing Application Integration.	125
Installing Application Integration interactively	125
Installing Application Integration silently	126
Verifying your Workplace Application Integration installation	127
Deploying multiple Application Engine instances	127
Deploying a second instance of Workplace	128
Deploying each additional Workplace instance as an EAR file	129
Enabling Application Engine to use ISRA	130
ISRA SSL support	131
Installing and deploying the Application Engine ISRA servlet.	131
Configuring Workplace site preferences for ISRA	133

Logging in to FileNet Image Services by using an LDAP account	133
Accessing FileNet Image Services library documents	134
Installing and configuring IBM System Dashboard for Enterprise Content Management	134
Installing the COM compatibility layer (CCL)	134

Part 2. Removing software 135

Removing the FileNet P8 documentation 137

Removing the FileNet P8 documentation from a WebSphere Application Server.	137
--	-----

Removing Content Platform Engine 139

Removing an entire Content Platform Engine installation interactively (AIX, HP/UX, Linux, Linux for System z, Solaris)	139
Removing Content Platform Engine silently	139
Removing data associated with Content Platform Engine	139

Removing IBM Content Search Services software 141

Removing IBM Content Search Services interactively	141
Removing IBM Content Search Services silently	141

Removing Application Engine (WebSphere). 143

Removing Rendition Engine 145

Removing the Application Engine ISRA servlet 147

Part 3. Appendixes 149

Appendix A. Configuration Manager reference 151

Overview of Configuration Manager	152
Configuration profile concepts.	152
Using the graphical and command-line user interfaces.	154
Gathering Configuration Manager values by using the Installation and Upgrade Worksheet	154
Handling passwords in Configuration Manager	155
Accessing the Configuration Manager log files	156
Correcting a dotnetclient configuration profile error	156
Adding an SSL signer to the Configuration Manager keystore (WebSphere)	157
Correcting an SSL Signer Exchange Prompt error (WebSphere).	158
Configuration Manager user interface reference	159
Starting Configuration Manager	159
Configuration Manager window	160

Main toolbar	160
Profile toolbar	161
Console toolbar.	161
Configuration Manager menus and commands	162
Working with Configuration Manager	165
Configuring a Content Platform Engine instance	166
Setting the password save preference	166
Creating a profile for a new installation	167
Creating a profile for an upgrade.	167
Opening and closing an existing profile or task	168
Editing the application server properties	169
Editing the properties for a specific task	169
Editing the Configure JDBC Data Sources tasks	169
Editing the Configure Login Modules task	170
Editing the Configure LDAP task.	170
Editing the Configure Bootstrap and Text Extraction task	171
Editing the Deploy Application task.	171
Applying the property settings by running a specific task	172
Applying the JDBC data source settings	172
Applying the login module settings	172
Applying the LDAP settings	173
Applying the bootstrap and text extraction settings	173
Deploying the application	173
Adding a task to a profile	174
Deleting a task from a profile	174
Running all tasks at the same time	175
Running a single task	175
Checking the task status.	175
Viewing the session log	176
Saving your changes to a task or profile	176
configmgr.ini parameters	176
Configuration Manager command-line reference	176
Running Configuration Manager commands	177
How to read the syntax diagrams	177
checkstatus command	178
execute command	182
generateconfig command	185
gui command	191
listtasks command	191
movetask command	194
removetask command	197
storepasswords command	200

Appendix B. Troubleshooting FileNet P8 installation and upgrade 203

Application server does not start after installation and shutdown (WebSphere Application Server)	203
Changing an incorrect value for the .NET API COM Compatibility Layer (CCL) server URL.	204
Changing the .NET API COM Compatibility Layer (CCL) server URL.	204

Notices 205

Trademarks	207
----------------------	-----

Index	209
------------------------	------------

ibm.com and related resources

Product support and documentation are available from [ibm.com](http://www.ibm.com).

Support and assistance

Product support is available on the Web. Click Support from the product Web site at:

FileNet Content Manager Support

<http://www.ibm.com/software/data/content-management/filenet-content-manager/support.html>

Information center

You can view the product documentation in an Eclipse-based information center that you can install when you install the product. By default, the information center runs in a Web server mode that other Web browsers can access. You can also run it locally on your workstation. See the information center at <http://publib.boulder.ibm.com/infocenter/p8docs/v5r2m0/index.jsp>.

PDF publications

You can view the PDF files online using the Adobe Acrobat Reader for your operating system. If you do not have the Acrobat Reader installed, you can download it from the Adobe Web site at <http://www.adobe.com>.

See the following PDF publications Web sites:

Product	Web site
Product Documentation for FileNet P8 Platform	http://www.ibm.com/support/docview.wss?rs=86&uid=swg27036786

"How to send your comments"

Your feedback is important in helping to provide the most accurate and highest quality information.

"Contacting IBM" on page viii

To contact IBM customer service in the United States or Canada, call 1-800-IBM-SERV (1-800-426-7378).

How to send your comments

Your feedback is important in helping to provide the most accurate and highest quality information.

Send your comments by using the online reader comment form at https://www14.software.ibm.com/webapp/iwm/web/signup.do?lang=en_US&source=swg-rcf.

Consumability survey

You are invited to tell IBM how to improve the consumability of software products. If you want to help IBM make IBM® FileNet® P8 easier to use, take the Consumability Survey at <http://www.ibm.com/software/data/info/consumability-survey/>.

Contacting IBM

To contact IBM customer service in the United States or Canada, call 1-800-IBM-SERV (1-800-426-7378).

To learn about available service options, call one of the following numbers:

- In the United States: 1-888-426-4343
- In Canada: 1-800-465-9600

For more information about how to contact IBM, see the Contact IBM Web site at <http://www.ibm.com/contact/us/>.

Part 1. Installing a distributed FileNet P8 system

To set up a FileNet P8 system you install and configure the software and documentation for a number of core components, including Content Platform Engine, Content Search Services, and Application Engine.

As an alternative to the Application Engine component and its Workplace user application, you can set up Workplace XT. If you are installing FileNet P8 for IBM Case Manager, you must install Workplace XT. See the Workplace XT documentation for details.

“Installing FileNet P8 documentation” on page 3

FileNet P8 documentation is distributed as part of a larger FileNet P8 information center. From the various user and administrative applications, you can either link to the online version of the information center on www.ibm.com or link to a local copy of the information center that you install and deploy.

“Installing and configuring Content Platform Engine” on page 9

Content Platform Engine is the content and workflow-management component of the FileNet P8 platform. To set up Content Platform Engine and get full workflow functionality, you install the Content Platform Engine and IBM Case Foundation software and then configure and deploy it on an application server. You must also configure the global configuration database (GCD), create the FileNet P8 domain, and create at least one object store with an associated workflow system. The workflow system contains an isolated region and an associated connection point. The GCD contains system information about your particular configuration. The object stores contain information about the documents, cases, records, forms, workflows, and other business objects that you store in your FileNet P8 system.

“Installing and configuring IBM Content Search Services” on page 65

You can install and configure IBM Content Search Services for a single server configuration or a multiple server configuration on Windows, AIX®, Linux, and Solaris operating systems.

“Installing and configuring Application Engine” on page 83

Application Engine provides a client application called Workplace that you can use to access the information managed by Content Platform Engine. After you install the server, you must also configure your application server to work with Application Engine, and deploy the application.

“Configuration and startup tasks” on page 113

After you install the FileNet P8 components, there are some additional steps to configure the system. After you configure the FileNet P8 components, familiarize yourself with system startup and shutdown procedures. See the **Administering FileNet P8 > Starting and stopping FileNet P8 components** help topic.

“Optional installation tasks” on page 123

You can install the additional or optional FileNet P8 components in any order.

Installing FileNet P8 documentation

FileNet P8 documentation is distributed as part of a larger FileNet P8 information center. From the various user and administrative applications, you can either link to the online version of the information center on www.ibm.com or link to a local copy of the information center that you install and deploy.

The advantages of linking to the [ibm.com](http://www.ibm.com) information center are:

- You do not have to maintain a documentation server and information center.
- You do not have to install any documentation in your environment, except for what is automatically installed within some of the FileNet P8 software components.
- The documentation is always up to date.

If you want to use the online information center, specify the base documentation URL for the online information center when you create the FileNet P8 domain or configure various user and administrative applications.

For more information about specifying the base documentation URL for either the online information center or a locally installed information center, see **Administering FileNet P8 > Administering Content Platform Engine > Getting started > Updating the base documentation URL for the FileNet P8 domain.**

If you want to access the documentation locally in your FileNet P8 environment, you must install and deploy the information center WAR file as a web application on a supported application server.

1. “Installing the local information center”
You can install interactively or silently and deploy the IBM FileNet P8 documentation as an information center. The information center documentation package is deployed as a WAR file on an application server.
2. “Starting and verifying the FileNet P8 information center” on page 6
After you install and deploy the FileNet P8 information center on the application server, verify that you can access its URL address and run its search feature. These tests ensure that the installed information center can be used as a help system in the various FileNet P8 component applications.
3. “Backing up and redeploying the FileNet P8 information center” on page 6
After you verify the installation of your FileNet P8 information center, you should store a backup copy. With a backup copy, you can more quickly recover from a disaster and redeploy to other servers.

Installing the local information center

You can install interactively or silently and deploy the IBM FileNet P8 documentation as an information center. The information center documentation package is deployed as a WAR file on an application server.

“Installing the FileNet P8 information center interactively” on page 4
You must install the FileNet P8 Platform information center as a Web application on a supported application server to view and search product documentation. When you install the information center interactively, you run a wizard that prompts you for an installation path for the information center WAR file.

“Installing the FileNet P8 information center silently” on page 5
You must install the FileNet P8 Platform information center as a Web application on a supported application server to view and search product documentation. When you install the information center silently, you run a command that references parameters in an installation text file.

Installing the FileNet P8 information center interactively

You must install the FileNet P8 Platform information center as a Web application on a supported application server to view and search product documentation. When you install the information center interactively, you run a wizard that prompts you for an installation path for the information center WAR file.

Before you install the FileNet P8 information center, you must ensure that you have Java™ support enabled on the application server you choose.

You can collocate the documentation information center on an application server with either Application Engine or Content Platform Engine server components installed. You can also install it on a separate application server.

Depending on your operating system and application server levels, your options might be slightly different from the options that are documented.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

To install the FileNet P8 information center interactively:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only documentation installation values, filter by **P8 Info Center Installer** in the **Installation or Configuration Program** column.

2. Log on to the application server where you are installing the information center:

Option	Description
AIX, HPUNIX, HPUNIXi, Linux, Linux for System z, Solaris	Log on as a user with read, write, and execute access to the directory where you plan to install the information center.

3. Access the information center software package.
4. Run the installation program:

Option	Description
Linux	5.2.0-P8IC-LINUX.BIN

5. Complete the installation program screens by using the values from your worksheet.
6. When the installation completes, check for errors in the information center error log file *ic_install_path/p8ic_install_log_5.2.0.txt*, where *ic_install_path* is the location where the information center p8docs.war file is installed.
7. Deploy the p8docs.war on your application server. The deployment might take several minutes because of the size of the documentation files.

Option	Description
WebSphere® Application Server	From the WebSphere administrative console, install the p8docs.war file as a Web application by using p8docs as the context root. Tip: In the configuration windows, you can accept the default values for all choices. In addition, ensure that you save to the primary configuration when prompted.

Installing the FileNet P8 information center silently

You must install the FileNet P8 Platform information center as a Web application on a supported application server to view and search product documentation. When you install the information center silently, you run a command that references parameters in an installation text file.

Before you install the FileNet P8 information center, you must ensure that you have Java support enabled on the application server you choose.

You can collocate the documentation information center on an application server with either Application Engine or Content Platform Engine server components installed. You can also install it on a separate application server.

Depending on your operating system and application server levels, your options might be slightly different from the options that are documented.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

To install the FileNet P8 Platform information center silently:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only documentation installation values, filter by **P8 Info Center Installer** in the **Installation or Configuration Program** column.

2. Log on to the application server where you are installing the information center:

Option	Description
AIX, HPUNIX, HPUNIXi, Linux, Linux for System z, Solaris	Log on as a user with read, write, and execute access to the directory where you plan to install the information center.

3. Access the information center software package.
4. Edit the p8ic_silent_install.txt file to reflect the installation choices in your worksheet.
5. Run one of the following commands, depending on your operating system:

Option	Description
Linux	5.2.0-P8IC-LINUX.BIN -f p8ic_silent_install.txt

- When the installation completes, check for errors in the information center error log file *ic_install_path/ic_install_log_5.2.0.txt*, where *ic_install_path* is the location where the information center *p8docs.war* file is installed.
- Deploy the *p8docs.war* on your application server. The deployment might take several minutes because of the size of the documentation files.

Option	Description
WebSphere Application Server	<ol style="list-style-type: none">Copy the FileNet P8 <i>p8docs.war</i> file to the local hard drive.From the WebSphere administrative console, install the <i>p8docs.war</i> file as a Web application by using <i>p8docs</i> as the context root. Tip: In the configuration windows, you can accept the default values for all choices. In addition, ensure that you save to the primary configuration when prompted.

Starting and verifying the FileNet P8 information center

After you install and deploy the FileNet P8 information center on the application server, verify that you can access its URL address and run its search feature. These tests ensure that the installed information center can be used as a help system in the various FileNet P8 component applications.

To verify the information center installation and deployment:

- From the application server, start the information center Web application named *p8docs*.
- From a Web browser, access the documentation URL by using the application server name and port number for your Web environment, for example:

Option	Description
IBM WebSphere Application Server	http://yourdocserver:9080/p8docs/index.jsp

Because of the size of the documentation package, the frames within the information center take a few minutes to load the first time.

- Make note of the base URL for your application server. You must enter the base URL as the documentation URL when you create a FileNet P8 domain by using Administration Console for Content Platform Engine. The base URL is <http://yourdocserver:port/p8docs/topic/>.
- Index the information center by performing a search. Indexing can take 5-10 minutes, and takes place automatically when the first search is performed.

Related information:

[acce_set_base_url](#)

Backing up and redeploying the FileNet P8 information center

After you verify the installation of your FileNet P8 information center, you should store a backup copy. With a backup copy, you can more quickly recover from a disaster and redeploy to other servers.

To back up your FileNet P8 information center for easy recovery or redeployment:

1. Create a `p8docs.war` or `p8docs` compressed file that contains the entire `p8docs` directory structure.
2. Place the file in a safe storage area that you can readily access to redeploy the FileNet P8 information center to new or updated application servers.

Installing and configuring Content Platform Engine

Content Platform Engine is the content and workflow-management component of the FileNet P8 platform. To set up Content Platform Engine and get full workflow functionality, you install the Content Platform Engine and IBM Case Foundation software and then configure and deploy it on an application server. You must also configure the global configuration database (GCD), create the FileNet P8 domain, and create at least one object store with an associated workflow system. The workflow system contains an isolated region and an associated connection point. The GCD contains system information about your particular configuration. The object stores contain information about the documents, cases, records, forms, workflows, and other business objects that you store in your FileNet P8 system.

All Content Platform Engine software is installed from the Content Platform Engine. Install IBM Case Foundation after installing Content Platform Engine. IBM Case Manager requires that both Content Platform Engine and IBM Case Foundation be installed.

You install the Content Platform Engine software and the IBM Case Foundation once on a web application server in your environment. You can configure and deploy one or more Content Platform Engine application instances on that server. A single Content Platform Engine application instance equates to one deployed application on your application server.

To deploy Content Platform Engine in a non-managed environment, you install and configure Content Platform Engine on a single server in the environment. After deploying the bootstrapped Content Platform Engine EAR file on the initial server, you copy the file to the other Configuration Manager profiles that are used to configure the other Content Platform Engine servers in the environment.

1. “Installing Content Platform Engine and IBM Case Foundation” on page 10
You must install the Content Platform Engine software to place the binary files for its components on the server. If you purchased IBM Case Foundation or will be installing IBM Case Manager, you must also install the IBM Case Foundation.
2. “Configuring Content Platform Engine” on page 17
You can configure and deploy all of your Content Platform Engine instances with Configuration Manager. Configuration Manager prepares the Content Platform Engine application for deployment on the application server. A single Content Platform Engine application instance equates to one deployed application on your application server.
3. “Deploying Content Platform Engine instances” on page 43
Depending on your environment, you can use the Configuration Manager graphical user interface, or the command line, to deploy Content Platform Engine instances.
4. “Installing storage device source files” on page 49
If your FileNet P8 system includes Tivoli® Storage Manager or EMC Centera devices, you must install files on the Content Platform Engine server.
5. “Configuring file stores for high availability” on page 54
File store content is managed from the Content Platform Engine application.

6. “Completing Content Platform Engine post-deployment steps” on page 54
You must complete the post-deployment web application server configuration before you can put a FileNet P8 system into production.
7. “Verifying the Content Platform Engine deployment” on page 55
You can verify that the Content Platform Engine deployment was successful by accessing the FileNet P8 System Health page.
8. “Creating the FileNet P8 domain” on page 58
You need to create a FileNet P8 domain to contain the object stores, storage areas, index areas, and other entities that you create.
9. “Creating a database connection” on page 58
You must create a database connection so that Content Platform Engine can connect to the database that is used by object stores and isolated regions.
10. “Creating the initial object store” on page 59
Object stores are used to store documents, workflows and other objects. The New Object Store wizard leads you through the steps required to create an object store.
11. “Creating a workflow system” on page 59
You must create a workflow system to contain your isolated regions. When you create a workflow system, you define an isolated region and its connection point. In addition, you can optionally customize the database storage parameters and configure email notification.
12. “Connecting to a highly available Content Platform Engine” on page 60
The configuration of the Content Platform Engine connection in a highly available environment depends on the type of application you want to connect to the Content Platform Engine. You can configure administrative applications or user applications to connect to Content Platform Engine.
13. “Verifying the Content Platform Engine system” on page 62
You can verify the Content Platform Engine system by using Administration Console for Content Platform Engine to create a folder in each object store.

Installing Content Platform Engine and IBM Case Foundation

You must install the Content Platform Engine software to place the binary files for its components on the server. If you purchased IBM Case Foundation or will be installing IBM Case Manager, you must also install the IBM Case Foundation.

1. “Installing Content Platform Engine” on page 11
You must install the Content Platform Engine software to place the software on the server. You can install the software interactively with a wizard or silently from the command line.
2. “Installing Enterprise Manager” on page 13
Install IBM FileNet Enterprise Manager on a Windows server to administer content in an enterprise content management system. You install this software by running the Content Platform Engine installation program on a supported Windows system.
3. “Installing Content Platform Engine software updates” on page 14
You must install the latest software updates, fix packs, or interim fixes for the Content Platform Engine software to ensure optimal operation.
4. “Installing IBM Case Foundation” on page 15
You can install IBM Case Foundation either interactively or silently.

Installing Content Platform Engine

You must install the Content Platform Engine software to place the software on the server. You can install the software interactively with a wizard or silently from the command line.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

Red Hat Enterprise Linux 5.1 (and later) has a security feature that can cause errors during installation. For details on resolving the issue before you install, see the *IBM(r) FileNet(r) P8 Hardware and Software Requirements*. In the guide, search for "SELinux".

You can install the Content Platform Engine components shown in the following table. Note that some of the components can be installed only on Windows. All installation procedures refer to using Administration Console for Content Platform Engine.

Enterprise Manager is being replaced by Administration Console for Content Platform Engine. Although Administration Console for Content Platform Engine has all required administration features, it does not yet have some of the functionality present in Enterprise Manager, for example adding documents with content or saving searches and search results. You can do these kinds of tasks through client applications such as IBM Content Navigator. The Administration Console for Content Platform Engine contains all the new administration features for this release and is the primary administration tool for the Content Platform Engine.

Table 1. Content Platform Engine components

Component	Description
Content Platform Engine	Install this software as the major Content Platform Engine component. When you install Content Platform Engine, Configuration Manager, tools, and Administration Console for Content Platform Engine are also installed.
.NET Clients (including Enterprise Manager)	Install this software only on client machines where you intend to run custom applications or on a Windows server where you intend to run Enterprise Manager.
Tools	Install tools on the Content Platform Engine server to get a number of tools for both content and workflow management use. Install tools if you need FileNet Deployment Manager. This tool is needed for IBM Case Manager configuration and it is available only on Windows and Linux configurations. You can also install only the tools on a workstation to get workflow system tools to run remotely from the Content Platform Engine server. Installation of either the Content Platform Engine server or the Content Platform Engine tools is a prerequisite to installation of IBM Case Foundation tools.

“Installing Content Platform Engine interactively”

To install Content Platform Engine software interactively, you run a wizard that prompts you for an installation path and the Content Platform Engine components to be installed.

“Installing Content Platform Engine silently” on page 13

When you install Content Platform Engine silently, you run a command in the Content Platform Engine software package that references parameters in an installation text file.

Related concepts:



Installation and upgrade worksheet

See the information about the worksheet in *Plan and Prepare Your Environment for IBM FileNet P8*.

Installing Content Platform Engine interactively

To install Content Platform Engine software interactively, you run a wizard that prompts you for an installation path and the Content Platform Engine components to be installed.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

To install Content Platform Engine:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Content Platform Engine values, filter by **CPE Installer** in the **Installation or Configuration Program** column.

2. Log on as `cpe_install_user` to the application server machine where you are going to install Content Platform Engine software.
3. Navigate to the Content Platform Engine software package in the installation media.
4. Run one of the following programs in the software package, depending on your operating system:

Platform	Command
Linux	5.2.0-P8CE-LINUX.BIN

5. Complete the Content Platform Engine installer screens by using the values from your worksheet.
6. Review the status messages in the final wizard screen, and close the wizard.
7. When the installation completes, click **Done** and check for errors in the Content Platform Engine `ce_install_path/ce_install_log_5.2.0.txt` error log file, where `ce_install_path` is the location where Content Platform Engine is installed. Also check the `ce_install_path/ce_install_summary.txt` file to see what components were installed.

Related concepts:

 [Installation and Upgrade Worksheet](#)

For more information about Content Engine parameter values, see *Plan and Prepare Your Environment for IBM FileNet P8*.

Installing Content Platform Engine silently

When you install Content Platform Engine silently, you run a command in the Content Platform Engine software package that references parameters in an installation text file.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

To install Content Platform Engine:

1. Open your completed Installation and Upgrade Worksheet file.


Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Content Platform Engine values, filter by **CPE Installer** in the **Installation or Configuration Program** column.

2. Log on as `cpe_install_user` to the application server machine where you are going to install Content Platform Engine software.
3. Navigate to the Content Platform Engine software package in the installation media.
4. Edit the `ce_silent_install.txt` file to reflect the installation choices in your worksheet.
5. Run one of the following commands in the software package, depending on your operating system:

Platform	Command
Linux	<code>5.2.0-P8CE-LINUX.BIN -i silent -f ce_silent_install.txt</code>

6. When the installation completes, check for errors in the Content Platform Engine error log file `ce_install_path/ce_install_log_5.2.0.txt`, where `ce_install_path` is the location where Content Platform Engine is installed. Also, check the `ce_install_path/ce_install_summary.txt` file to see a list of the components that were installed.

Related concepts:

 [Installation and upgrade worksheet](#)

For more information about the installation and upgrade worksheet, see the worksheet topics in *Plan and Prepare Your Environment for IBM FileNet P8*.

Installing Enterprise Manager

Install IBM FileNet Enterprise Manager on a Windows server to administer content in an enterprise content management system. You install this software by running the Content Platform Engine installation program on a supported Windows system.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

If you did not install Enterprise Manager when you installed the Content Platform Engine software, you can install it now on the same Windows server or on some other Windows computer.

Tip: An icon labeled **FileNet Enterprise Manager Administration Tool** on the desktop of the Content Platform Engine server indicates that Enterprise Manager has been installed.

Important: You can only install Enterprise Manager on a Windows machine.

To install Enterprise Manager:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Content Platform Engine values, filter by **CPE Installer** in the **Installation or Configuration Program** column.

2. On the machine where you install Enterprise Manager, log on as a member of the Local Administrators group or the Power® Users group.
3. If you have not already done so, install the required prerequisite software for the Enterprise Manager. The prerequisites are .NET 3.0 or WSE 3.0.
4. Access the Content Platform Engine software package.
5. Start the Enterprise Manager installation.

Option	Description
To install interactively	<ol style="list-style-type: none">1. Run the following command in the software package: 5.2.0-P8CE-WIN.exe.2. Complete the installation program wizard.
To install silently	<ol style="list-style-type: none">1. Open the ce_silent_install.txt file in the software package for editing.2. Set the parameter values in the ce_silent_install.txt file for your site. Be sure to set the CHOSEN_INSTALL_FEATURE_LIST parameter value to: DotNetClients,AdminTools3. Save your edits.4. Run the following command in the software package on a single line: 5.2.0-P8CE-WIN.EXE -i silent -f ce_silent_install.txt

Installing Content Platform Engine software updates

You must install the latest software updates, fix packs, or interim fixes for the Content Platform Engine software to ensure optimal operation.

If no Content Platform Engine software updates are available, skip this procedure.

To install the Content Platform Engine software updates:

1. Access the FileNet P8 support site to obtain the latest Content Platform Engine software updates.
2. Open the readmes for the Content Platform Engine software updates and perform the installation procedures in the readmes on each Content Platform Engine instance.

Related information:



IBM FileNet P8 Platform documentation and support

Obtain the latest Content Platform Engine software updates, as well as the rest of the IBM FileNet P8 Platform documentation.

Installing IBM Case Foundation

You can install IBM Case Foundation either interactively or silently.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

You can install the IBM Case Foundation components shown in the following table. Note that some of the components can be installed only on Windows.

Table 2. IBM Case Foundation components

Component	Description
IBM Case Foundation	Install this software on a Content Platform Engine to enable full workflow processing capabilities.
Tools	Install the tools on the Content Platform Engine server after installing the Content Platform Engine server. Alternatively, install only the Content Platform Engine tools on a remote workstations, then install the IBM Case Foundation tools.
Case Analyzer Components	Choose from the Case Analyzer components. Excel and SSAS OLAP options only appear on Microsoft Windows platforms. See the <i>IBM FileNet Case Analyzer Installation and Upgrade Guide</i> for more information.

“Installing IBM Case Foundation interactively”

Use these procedures to install IBM Case Foundation using the installation wizard screens included with the installation package.

“Installing IBM Case Foundation silently” on page 16

Modify the silent installation response file according to the values in the installation worksheet before installing the software.

Installing IBM Case Foundation interactively

Use these procedures to install IBM Case Foundation using the installation wizard screens included with the installation package.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only IBM Case Foundation values, filter by **CF Installer** in the **Installation or Configuration Program** column.

2. Log on as *cpe_install_user* to the application server machine where you are going to install IBM Case Foundation software.
3. Navigate to the IBM Case Foundation software package in the installation media.
4. Run one of the following programs in the software package, depending on your operating system:

Platform	Command
Linux	5.2.0-P8CaseFoundation-LINUX.BIN

5. Complete the IBM Case Foundation installer screens by using the values from your worksheet.
6. Review the status messages in the final wizard screen, and close the wizard.
7. When the installation completes, check for errors in the IBM Case Foundation log file *case_foundation_install_path/casefoundation_install_log_5.2.0.txt*, where *case_foundation_install_path* is the location where IBM Case Foundation is installed. Also check the file *case_foundation_install_path/caseFoundation_install_summary.txt* to see a summary of the installation.

Installing IBM Case Foundation silently

Modify the silent installation response file according to the values in the installation worksheet before installing the software.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only IBM Case Foundation values, filter by **CF Installer** in the **Installation or Configuration Program** column.

2. Log on as *cpe_install_user* to the application server machine where you are going to install IBM Case Foundation software.
3. Navigate to the IBM Case Foundation software package in the installation media.
4. Edit the *CaseFoundation_silent_install.txt* file to reflect the installation choices in your worksheet.
5. Run one of the following commands in the software package, depending on your operating system:

Platform	Command
Linux	5.2.0-P8CaseFoundation-LINUX.BIN -i silent -f CaseFoundation_silent_install.txt

6. When the installation completes, check for errors in the IBM Case Foundation log file *case_foundation_install_path/casefoundation_install_log_5.2.0.txt*, where *case_foundation_install_path* is the location where IBM Case Foundation is installed. Also check the file *case_foundation_install_path/caseFoundation_install_summary.txt* to see a summary of the installation.

Configuring Content Platform Engine

You can configure and deploy all of your Content Platform Engine instances with Configuration Manager. Configuration Manager prepares the Content Platform Engine application for deployment on the application server. A single Content Platform Engine application instance equates to one deployed application on your application server.

Configuration is a multiple step process. You must provide information about your Content Platform Engine application environment, apply the settings by running the configuration tasks, and deploy the application. You can configure multiple instances before you deploy any of them, or you can configure and deploy one instance at a time.

You use Configuration Manager to define the following information for the Content Platform Engine instance:

- Application server properties
- Java Database Connectivity (JDBC) data source properties for the global configuration database (GCD) database
- Java Database Connectivity (JDBC) data source properties for each object store database
- Directory service (LDAP) provider properties
- Content Platform Engine application login modules
- Content Platform Engine bootstrap properties

Remember the following points when you prepare to configure Content Platform Engine:

- You can use Configuration Manager to configure and deploy the Content Platform Engine software that you installed on an application server only if Configuration Manager is running with the same application server.
 - (WebSphere Application Server only) For best results, configure no more than one Content Platform Engine application instance in a WebSphere profile.
 - (WebSphere Application Server only) Configuration Manager can connect to a remote WebSphere Application Server stand-alone server or Network Deployment Manager if a matching WebSphere Application Server installation is available where Configuration Manager runs.
 - If you need an accessible software version of Configuration Manager for people with disabilities, use the command-line version of Configuration Manager.
 - If your FileNet P8 domain uses multiple non-managed application servers, then you must repeat all Configuration Manager tasks, except the Configure Bootstrap and Text Extraction task, on each non-managed application server. For the Configure Bootstrap and Text Extraction task, copy a single EAR file with the bootstrap settings to the Configuration Manager profiles that configure the other Content Platform Engine servers in the environment.
1. "Granting directory permissions to the Configuration Manager user" on page 18
You must grant file and directory permissions to *config_mgr_user*, which is the user who runs Configuration Manager, to allow this user to run the program and create files in the *ce_install_path/tools/configure* directory.
 2. "Configuring Content Platform Engine instances" on page 18
You can configure and deploy all of your Content Platform Engine application instances with Configuration Manager. A single Content Platform Engine

application instance equates to one deployed application on your application server. You can use the graphical user interface or the command-line interface for Configuration Manager.

Granting directory permissions to the Configuration Manager user

You must grant file and directory permissions to *config_mgr_user*, which is the user who runs Configuration Manager, to allow this user to run the program and create files in the *ce_install_path/tools/configure* directory.

To grant permissions to the Configuration Manager user:

1. If you are doing a new installation or upgrading on a new machine where Content Engine has never been installed, log on as the *cpe_install_user*. If you are upgrading on the same machine where Content Engine was previously installed, log on as the same user who originally installed that software. The installation program requires this to detect that it is an upgrade and to use the same installation path.
2. Grant permissions to the *config_mgr_user* user for the executable file that you intend to use:

Option	Description
AIX, Solaris, HPUX, HPUXi, Linux, Linux for System z - graphical user interface	Grant execute permission to configmgr
AIX, Solaris, HPUX, HPUXi, Linux, Linux for System z - command line	Grant execute permission to configmgr_cl

3. Grant write permission to the directory where you want Configuration Manager to place the configuration XML files that it creates.
If you do not specify the profile directory when you run Configuration Manager, grant write permission on the default directory *ce_install_path/tools/configure* and all its files and subdirectories.
4. Log off the Content Platform Engine server and log on again as *config_mgr_user*.

Related tasks:

 IBM FileNet P8 accounts

See the P8 account information for details on how to specify the required accounts and their permissions in the *Plan and Prepare Your Environment for IBM FileNet P8*.

Configuring Content Platform Engine instances

You can configure and deploy all of your Content Platform Engine application instances with Configuration Manager. A single Content Platform Engine application instance equates to one deployed application on your application server. You can use the graphical user interface or the command-line interface for Configuration Manager.

Before starting Configuration Manager, ensure that the application server is running or stopped, depending on its type:

Option	Description
WebSphere Application Server	Start the application server if it is not already running.

“Configuring Content Platform Engine instances by using the graphical user interface”

You use the graphical user interface version of Configuration Manager to configure and deploy a Content Platform Engine application instance on an application server.

“Configuring instances by using the command line” on page 27

You can configure a Content Platform Engine instance on a web application server by using the command-line version of Configuration Manager.

Configuring Content Platform Engine instances by using the graphical user interface

You use the graphical user interface version of Configuration Manager to configure and deploy a Content Platform Engine application instance on an application server.

First, you create a configuration profile that defines:

- The JDBC data source settings
- The login modules for the Content Platform Engine application
- The directory service provider (LDAP) settings
- The Content Platform Engine bootstrap settings

You can follow the recommended order to edit and run the individual configuration tasks. However, you can edit and run the Configure GCD JDBC Data Sources, Configure Object Store JDBC Data Sources, Configure Login Modules, Configure LDAP properties, and Configure Bootstrap and Text Extraction tasks in any order. You do not need to complete work on one configuration task before starting another. You can save your edits, switch between tasks, close the tasks, and reopen tasks as needed. However, you must complete all of these tasks before you deploy the application.

1. “Starting the Configuration Manager graphical user interface” on page 20
You can start the graphical interface version of Configuration Manager to configure a Content Platform Engine application instance on a web application server.
2. “Changing the password save preference” on page 20
By default, any passwords that you enter in the graphical user interface in Configuration Manager are not saved to a file. The passwords are stored in memory as long as you have the profile open in Configuration Manager. You can change the password save preference to save the passwords each time that you save your changes to a profile.
3. “Creating a new configuration profile” on page 21
Configuration Manager stores your settings for deploying a Content Platform Engine application instance in a configuration profile. The profile defines the application server settings, the JDBC data source settings, the login modules settings, the directory service provider (LDAP) settings, the Content Platform Engine bootstrap settings, and the application deployment settings. You must create a new profile for each Content Platform Engine instance that you are configuring.
4. “Configuring the global configuration database JDBC data source settings” on page 22
You must provide property information about the JDBC data sources for the global configuration database (GCD). Content Platform Engine uses the data source information to connect to and update the GCD.
5. “Configuring the initial object store data sources by using the graphical user interface” on page 23

Content Platform Engine uses the data source information to connect to and update the object store database. By default, each profile includes a task for creating the data sources for an object store.

6. “Configuring the login modules (WebSphere and JBoss only)” on page 24
You must configure the login modules for the Content Platform Engine application. The login modules provide authentication information for the Content Platform Engine application.
7. “Configuring Content Platform Engine application server authentication (LDAP) settings” on page 25
You must configure the Content Platform Engine application server's authentication settings. These settings define the (LDAP) repository and search mechanism, which the application server uses to authenticate a user requesting Content Platform Engine service.
8. “Configuring bootstrap and text extraction settings” on page 26
The bootstrap settings are for creating the global configuration database (GCD) and for starting Content Platform Engine. The text extraction setting is needed for updating the Content Platform Engine EAR file with the IBM Content Search Services API JAR files and text extraction modules.

Starting the Configuration Manager graphical user interface:

You can start the graphical interface version of Configuration Manager to configure a Content Platform Engine application instance on a web application server.

See the appendix “Configuration Manager user interface reference” on page 159 for complete information about using the graphical user interface. If you need an accessible version of Configuration Manager, use the command-line interface instead of the graphical user interface.

To start Configuration Manager:

1. Start Configuration Manager by running one of the following commands, depending on the operating system that runs on the machine where you installed Content Platform Engine, and log on as the *config_mgr_user*:

Option	Description
AIX, Solaris, HPUNIX, HPUNIXi, Linux, Linux for System z	Run this command: <code>ce_install_path/tools/configure/configmgr</code>

The first time that you start Configuration Manager, the Welcome is displayed.

2. Select one of the links in the Welcome to learn more or to start working in a wizard, or close the Welcome by clicking the **X** in the tab at the upper left. You can reopen the Welcome later, as needed, from the **Help** menu.

Changing the password save preference:

By default, any passwords that you enter in the graphical user interface in Configuration Manager are not saved to a file. The passwords are stored in memory as long as you have the profile open in Configuration Manager. You can change the password save preference to save the passwords each time that you save your changes to a profile.

When you close the profile, the passwords are erased from memory. Each time that you start Configuration Manager or open a saved profile, the passwords are blank (unless you previously changed the preferences setting). Before you can run a task, you must specify the passwords required by the task and the application server

properties; otherwise, the task will not run successfully. If your site security requirements permit you to save passwords to a file, you can change the password save preference setting.

To change the password save preference:

1. Click **Window > Preferences**.
2. Complete one of the following actions:

Option	Description
To save passwords to file	Select the Save all passwords to file when saving a task or profile check box.
To prevent writing passwords to file	Clear the Save all passwords to file when saving a task or profile check box.

3. Click **OK**.

Creating a new configuration profile:

Configuration Manager stores your settings for deploying a Content Platform Engine application instance in a configuration profile. The profile defines the application server settings, the JDBC data source settings, the login modules settings, the directory service provider (LDAP) settings, the Content Platform Engine bootstrap settings, and the application deployment settings. You must create a new profile for each Content Platform Engine instance that you are configuring.

The information for a profile is collected in XML files in the form of properties and values that describe the associated configuration and deployment tasks. You must provide values for the profile properties that are specific to each configuration at your site, such as the application server name. The XML files are stored in a directory that is unique to a given profile. Because the profile name is used for the directory name and for the configuration profile file name, you must provide a profile name that is a valid directory name for your operating system. By default, the profiles are stored in the *ce_install_path*/tools/configure/profiles directory, where *ce_install_path* is the location where Content Platform Engine is installed. For more information on profiles, see “Configuration profile concepts” on page 152.

Tip: For more information on the properties and values that you set in Configuration Manager, roll your mouse over the property name to view the tool tip help for the property.

To create a configuration profile:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Configuration Manager values, filter by **CM: Create New Installation Profile** in the **Installation or Configuration Program** column.


2. Start the Create New Installation Profile wizard by selecting **File > New Installation Profile**.
3. Complete the wizard screens by using the values in your worksheet.

Attention: WebSphere Application Server and Oracle WebLogic Server: If you are creating the profile for a highly available clustered environment, use the profile for the WebSphere Application Server deployment manager, or the domain for the Oracle WebLogic Server administrative server.

- Optional: WebSphere Application Server and Oracle WebLogic Server only. In the Set Properties for Application Server screen, click **Test Connection** to test the connection between Configuration Manager and the application server by using the information that you provided. The test is optional, and you can proceed in the wizard even if the test fails. If the test fails, make sure that the application server is running and that the application server property values that you entered match the values that are defined in your application server.

The profile you created is displayed as an icon in the profile pane (left pane), along with icons for the tasks you selected. By default, the **Deploy Application** task is disabled. You must enable the task later in the configuration process.

Related concepts:

 Installation and upgrade worksheet

For more information about the installation and upgrade worksheet, see the worksheet topics in *Plan and Prepare Your Environment for IBM FileNet P8*.

Configuring the global configuration database JDBC data source settings:

You must provide property information about the JDBC data sources for the global configuration database (GCD). Content Platform Engine uses the data source information to connect to and update the GCD.

Ensure that the application server instance is running or stopped, depending on its type:

Table 3. Required application server state

Option	Description
WebSphere Application Server	Start the application server instance if it is not already running.

To configure the JDBC settings:


- Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Configuration Manager values, filter by **CM: Configure GCD JDBC Data Sources** in the **Installation or Configuration Program** column.

- If your configuration profile is not open in Configuration Manager, open the profile.
- Right-click **Configure GCD JDBC Data Sources** in the profile pane and select **Edit Selected Task**.
- Enter the property values for your database by using the values in your worksheet.
- Optional: (WebSphere and WebLogic only) Click **Test Database Connection** to test the connection to the database by using the database user name, database server name, database name, port number, and password that you provided. The test does not create the data sources.
 - Start the WebLogic Server administrative console.
 - Click **Lock & Edit > Services > Data Sources**.
 - Select the check box for the data source and then click **Delete**.
 - Click **Activate Changes**.
- Click **Save** to save your changes.

7. Ensure that the task is enabled. When the task is disabled, the task name includes the text **(disabled)**. To enable the task, select **Configure GCD JDBC Data Sources (disabled)** in the profile pane, and then either right-click and choose **Enable Selected Task** from the context menu, or click the **Enable the Selected Task** icon in the task toolbar.
8. Apply the JDBC property settings by right-clicking **Configure GCD JDBC Data Sources** in the profile pane, and selecting **Run Task**. Running the configuration task can take several minutes. The task execution status messages are displayed in the console pane below the JDBC properties.
9. Close the Configure GCD JDBC Data Sources task pane. In this step, you created the GCD data sources. You create the initial object store data sources later in the configuration process.

Related concepts:

 Installation and upgrade worksheet

For more information about the installation and upgrade worksheet, see the worksheet topics in *Plan and Prepare Your Environment for IBM FileNet P8*.

Configuring the initial object store data sources by using the graphical user interface:

Content Platform Engine uses the data source information to connect to and update the object store database. By default, each profile includes a task for creating the data sources for an object store.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

Tip: For more information about the properties and values you set in Configuration Manager, roll your mouse over the property name to view its hover help.

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that you enabled the **Data > Filter > AutoFilter** command. To view only Configuration Manager values for this task, filter by **CM: Configure Object Store JDBC Data Sources (object store 1)** in the **Installation or Configuration Program** column.

2. Start or stop the application server, depending on its type.

Table 4. Required application server operation


Application server type	Operation
WebSphere Application Server	Start the application server instance if it is not already running.

3. If your configuration profile is not open in Configuration Manager, open it by selecting **File > Open** and navigating to your *profilename.cfgp* file.
4. Right-click **Configure Object Store JDBC Data Sources** in the profile pane, and select **Edit Selected Task**.
5. Enter the property values for your data sources by using the values in your installation worksheet.
6. Click **Save** to save your changes.
7. Optional: WebSphere and WebLogic only. Click **Test Database Connection** to test the connection to the database by using the database user name, database

server name, database name, port number, and password that you provided. The test does not create the data sources.

8. Ensure that you enabled the task. When the task is disabled, the task name includes the text **(disabled)**. To enable the task, right-click **Configure Object Store JDBC Data Sources (disabled)** in the profile pane, and choose **Enable Selected Task** from the menu.
9. Apply the JDBC property settings by right-clicking **Configure Object Store JDBC Data Sources** in the profile pane, and selecting **Run Task**. Running the configuration task can take several minutes. The system displays the task execution status messages in the Console pane.

Related concepts:

 Installation and upgrade worksheet

For more information about the installation and upgrade worksheet, see the worksheet topics in *Plan and Prepare Your Environment for IBM FileNet P8*.

Related tasks:

“Creating a new configuration profile” on page 21

Configuration Manager stores your settings for deploying a Content Platform Engine application instance in a configuration profile. The profile defines the application server settings, the JDBC data source settings, the login modules settings, the directory service provider (LDAP) settings, the Content Platform Engine bootstrap settings, and the application deployment settings. You must create a new profile for each Content Platform Engine instance that you are configuring.

Starting or stopping an application server instance

Configuring the login modules (WebSphere and JBoss only):

You must configure the login modules for the Content Platform Engine application. The login modules provide authentication information for the Content Platform Engine application.

Ensure that the application server instance is running or stopped, depending on its type:

Table 5. Required application server state

Option	Description
WebSphere Application Server	Start the application server instance if it is not already running.

To configure the login module settings:

1. If your configuration profile is not open in Configuration Manager, open the profile.
2. If the Configure Login Modules task does not exist in the profile, add the task. Ensure that the task is enabled. When the task is disabled, the task name includes the text **(disabled)**. To enable the task, select **Configure Login Modules (disabled)** in the profile pane, and then either right-click and choose **Enable Selected Task** from the context menu, or click the **Enable the Selected Task** icon in the task toolbar.
3. Create the login modules by right-clicking **Configure Login Modules** in the profile pane, and selecting **Run Task**. Running the configuration task can take several minutes. The task execution status messages are displayed in the console pane below the login modules properties.

4. Close the Configure Login Modules task pane.

Related tasks:

Starting or stopping an application server instance

Configuring Content Platform Engine application server authentication (LDAP) settings:

You must configure the Content Platform Engine application server's authentication settings. These settings define the (LDAP) repository and search mechanism, which the application server uses to authenticate a user requesting Content Platform Engine service.

Important: Be aware that the changes you make to directory service provider settings overwrite the global security settings in the application server where Content Platform Engine is to be deployed. Run the Configure LDAP task only if you need to change the security settings.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

If you plan to configure Content Platform Engine to use the directory server's e-mail attribute or, for Active Directory, the userPrincipalName (UPN) to be the user short name used for login, then you must perform additional configuration steps and enter specific values for your LDAP settings. For detailed steps, see the IBM FileNet P8 help topic **Security > IBM FileNet P8 security > How to... > Configure Content Engine to use e-mail or UPN for login**.

Manual procedures to configure multiple realms for application server authentication can be found in the IBM FileNet P8 help topic **Security > IBM FileNet P8 Security > How to... > Configure multiple realms**.

To configure the LDAP settings:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Configuration Manager values, filter by **CM: Configure LDAP** in the **Installation or Configuration Program** column.

2. If your configuration profile is not open in Configuration Manager, open the profile.
3. Enter property values for the LDAP provider:
 - a. Right-click **Configure LDAP** in the profile pane, and select **Edit Selected Task**.
 - b. Enter the property values for your LDAP provider, by referring to the values from your worksheet.
4. Optional: (WebSphere and WebLogic only) Click **Test LDAP Connection** to test the connection to the directory service provider by using the directory service bind user name, host name, port number, and password that you provided.
5. Click **Save** to save your changes.
6. Ensure that the task is enabled. When the task is disabled, the task name includes the text **(disabled)**. To enable the task, select **Configure LDAP (disabled)** in the profile pane, and then either right-click and choose **Enable Selected Task** from the context menu, or click the **Enable the Selected Task** icon in the task toolbar.

7. Apply the LDAP property settings by right-clicking **Configure LDAP** in the profile pane and selecting **Run Task**. Running the configuration task can take several minutes. The task execution status messages are displayed in the console pane below the LDAP properties.
8. Close the Configure LDAP task pane.

Related concepts:



Installation and upgrade worksheet

For more information about the installation and upgrade worksheet, see the worksheet topics in *Plan and Prepare Your Environment for IBM FileNet P8*.

Configuring bootstrap and text extraction settings:

The bootstrap settings are for creating the global configuration database (GCD) and for starting Content Platform Engine. The text extraction setting is needed for updating the Content Platform Engine EAR file with the IBM Content Search Services API JAR files and text extraction modules.

Be sure that you have available the Installation and Upgrade Worksheet that was filled out during your planning activities.

If your FileNet P8 domain uses multiple non-managed application servers, then complete this procedure only on the initial server. You use a copy of the same EAR file with the bootstrap settings on all the servers.

To edit the bootstrap and text extraction settings:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Configuration Manager values, filter by **CM: Configure bootstrap properties** in the **Installation or Configuration Program** column.

2. If your configuration profile is not open in Configuration Manager, open the profile.
3. Right-click **Configure Bootstrap Properties and Text Extraction** in the profile pane and select **Edit Selected Task**.
4. In the **Bootstrap operation** field, select **Configure New**.
5. Enter the property values for your database by using the values in your worksheet.
6. Click **File > Save** to save your changes.
7. Ensure that the task is enabled. When the task is disabled, the task name includes the text **(disabled)**. To enable the task, select **Configure Bootstrap and Text Extraction (disabled)** in the profile pane, and then right-click and choose **Enable Task** from the context menu.
8. Apply the bootstrap property settings by right-clicking **Configure Bootstrap and Text Extraction** in the profile pane, and select **Run Task**. Running the configuration task can take a few minutes. The task execution status messages are displayed in the console pane below the bootstrap properties.
9. Optional: Click **View Bootstrapped EAR Information** to display the bootstrap information from the modified EAR file.
10. Close the Configure Bootstrap Properties and Text Extraction task pane.
11. If your FileNet P8 domain uses multiple non-managed application servers, then copy the `ce_install_path/ContentEngine/tools/configure/profiles/`

`my_profile/ear/Engine-app_server_type.ear` file to the profiles directory on each additional Content Platform Engine server.

`ce_install_path`

The location where Content Platform Engine is installed.

`my_profile`

The directory for the Configuration Manager profile that you created.

Engine-app_server_type.ear

The EAR file for your application server type: Engine-ws.ear, Engine-wl.ear, or Engine-jb.ear.

Important: Run the **Configure Bootstrap and Text Extraction** task only on the initial server.

Related concepts:



Installation and upgrade worksheet

For more information about the installation and upgrade worksheet, see the worksheet topics in *Plan and Prepare Your Environment for IBM FileNet P8*.

Configuring instances by using the command line

You can configure a Content Platform Engine instance on a web application server by using the command-line version of Configuration Manager.

Begin by generating the configuration XML files that define the application server settings, the global configuration database (GCD) data source JDBC data source settings, the login modules for the Content Platform Engine application, the directory service provider (LDAP) settings, and the Content Platform Engine bootstrap settings. Next, edit the files to provide values for your environment. Then, apply the settings by executing the tasks from a command prompt.

You must generate, edit, and run a complete set of configuration XML to configure a Content Platform Engine application. If you are deploying multiple Content Platform Engine application instances on the same application server, you must generate, edit, and deploy a complete set of configuration files for each instance. Store the configuration files for each instance in a separate directory.

You can complete the configuration tasks by generating all the configuration XML files before editing, running, or verifying any of them; or you can generate, edit, run, and verify one file at a time.

1. “Generating the configuration XML files for a Content Platform Engine instance” on page 28
The configuration XML files contain the properties and values for the various configuration tasks. From the command line, you can generate all of the XML files at the same time, or you can generate a single configuration XML file at a time.
2. “Creating the data sources by using the command line” on page 32
You must create the JDBC data sources for each object store that Content Platform Engine uses. You must generate, edit, and execute a new `configurejdbcos.xml` file for each object store in your environment.
3. “Editing the configuration XML files for a Content Platform Engine instance” on page 34
You must edit each configuration XML file to provide the property values for your environment. You can use any text editor to open and edit the files.

4. “Running the configuration XML files” on page 37
Running the configuration XML files applies the settings. You use the **execute** command to apply your configuration settings from the command line.
5. “Checking the completion status of Content Platform Engine configuration tasks” on page 41
Task execution messages are displayed in the console when you run a task, and you can view the status of a specific task at any time by running the **checkStatus** command. From the command line, you can check the status of all the configuration tasks or check the status of a single task.

Generating the configuration XML files for a Content Platform Engine instance:

The configuration XML files contain the properties and values for the various configuration tasks. From the command line, you can generate all of the XML files at the same time, or you can generate a single configuration XML file at a time.

The following table lists the configuration XML files that you need to generate to configure a new Content Platform Engine instance.

Table 6. Configuration XML files

File Name	Description
applicationserver.xml	Settings for the application server, including the location of the application server software and the name of the server. This file is generated when any other configuration file is generated (either all at the same time or individually) and is used by all of the configuration tasks. If you generate the files one at a time, this file is created only once.
configurebootstrap.xml	Settings for creating the global configuration database (GCD) and starting Content Platform Engine.
configurejdbcgcd.xml	Settings for configuring JDBC connections to the databases used by Content Platform Engine. You must generate, edit, and run the configure the JDBC task once for the data sources for the global configuration database (GCD) and then again for the data sources for each object store and Process Engine database. For information about creating the additional data sources for an object store or workflow system, see “Creating the data sources by using the command line” on page 32.
configurejdbcos.xml	
configurejdbcos. <i>n</i> .xml , where <i>n</i> is an integer starting with 2	
	If you generate a second JDBC configuration file, then it is named configurejdbc.2.xml. The file name increments for each new file that you generate.
configureldap.xml	Settings for connecting to and searching within a directory server. If your site uses multiple LDAP providers, you can generate an additional file for each provider. If you generate a second LDAP configuration file, then it is named configureldap.2.xml. The file name increments for each new file that you generate.
configureldap. <i>n</i> .xml , where <i>n</i> is an integer starting with 2	

Table 6. Configuration XML files (continued)

File Name	Description
configureloginmodules.xml	Settings for creating the application server login modules for Content Platform Engine.

You must eventually generate each of the required configuration XML files to configure a Content Platform Engine instance.

“Generating all of the configuration XML files at the same time”

From the command line, you can generate all of the required configuration XML files for Content Platform Engine at the same time with a single command.

“Generating one configuration XML file at a time (WebSphere)” on page 31

From the command line, you can generate each of the required configuration XML files for Content Platform Engine one file at a time.

Generating all of the configuration XML files at the same time:

From the command line, you can generate all of the required configuration XML files for Content Platform Engine at the same time with a single command.

When you run the **generateconfig** command, all the required configuration XML files are created.

To generate all the configuration XML files at the same time:

1. Log on to the Content Platform Engine server as *config_mgr_user*, the user who runs Configuration Manager.
2. Change the current directory to *ce_install_path/tools/configure*, where *ce_install_path* is the location where the Content Platform Engine software is installed.
3. Run the following command. Do not type any line breaks when you enter the command.

WebSphere Application Server

```
configmgr_cl generateconfig -appserver app_server_type
-repositorytype ldap_repository_type
-db db_type -ldap ldap_type
-bootstrap bootstrap_operation
-deploy deploy_type -profile myprofile
```

Where:

-appserver *appserver_name*

The **-appserver** *appserver_type* parameter specifies the type of application server and must be WebSphere, WebLogic, or JBoss.

-repositorytype *ldap_repository_type*

WebSphere Application Server only. The **-repositorytype** *ldap_repository_type* parameter specifies the type of LDAP repository to use and must be standalone or federated.

-db *database_type*

The **-db** *database_type* parameter is required only when you are generating all the files at the same time or when you are generating a single file by using the *configurejdbcgcd* option or the *configurejdbcos* option. This parameter specifies the type of database to be used by Content Platform Engine and must be mssql, oracle, oracle_rac, db2, or db2zos.

-ldap *ldap_type*

The **-ldap** *ldap_type* parameter is required only when you are generating all the files at the same time or when you are generating a single file by using the `configureldap` option. This parameter specifies the type of directory service repository that Content Platform Engine uses for authenticating users and must be `activedirectory`, `adam`, `ca`, `edirectory`, `oid`, `oracledirectoryse`, or `tivoli`. The `adam` value applies to both Microsoft ADAM and AD LDS.

-bootstrap *bootstrap_operation*

The **-bootstrap** *bootstrap_operation* parameter is required only when you are generating all the files at the same time or when you are generating a single file by using the `configurebootstrap` option. This parameter specifies the bootstrap and text extraction operation for the profile and must be `new`, `modify`, or `upgrade`.

-deploy *deploy_type*

The **-deploy** *deploy_type* parameter is required only when you are generating all the files at the same time or when you are generating a single file by using the `deployapplication` option. This parameter specifies the type of Content Platform Engine deployment. The value must be `standard`, `cluster`, or `netdeploy` (network deployment).

Specify `standard` if you are deploying Content Platform Engine to a stand-alone (that is, a server that is neither managed nor clustered) WebSphere Application Server, Oracle WebLogic Server, or JBoss Application Server.

Specify `cluster` if you are deploying Content Platform Engine to a WebSphere Application Server, Oracle WebLogic Server, or JBoss Application Server cluster.

Specify `netdeploy` if you are deploying Content Platform Engine to a managed WebSphere Application Server instance. That is, you are using Network Deployment to manage individual servers that are not in a cluster.

-profile *myprofile*

The **-profile** *myprofile* parameter specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as `ce_was_tiv_db2`. The profile must be located in the `ce_install_path/tools/configure/profiles` directory, where `ce_install_path` is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2"` or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2`.
- The fully qualified path to the profile input file, such as `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg"` or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg`.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg"`.

For example, the following command generates all the configuration XML files for a new installation profile for a standard deployment on WebSphere with IBM Tivoli Directory Server that uses a stand-alone LDAP repository and DB2® in the *ce_install_path/tools/configure/profiles/wstdb2* directory:

```
configmgr_cl generateconfig -appserver WebSphere
-repositorytype standalone -db db2 -ldap tivoli
-bootstrap new -deploy standard -profile wstdb2
```

Generating one configuration XML file at a time (WebSphere):

From the command line, you can generate each of the required configuration XML files for Content Platform Engine one file at a time.

You must generate the configuration XML files for each of these required configuration tasks:

- Create the XML file for the bootstrap properties file by using the `configurebootstrap` option.
 - Create the XML file for configuring the JDBC Data Sources for the global configuration database (GCD) database by using the `configurejdbcgcd` option.
 - Create the XML file for configuring the JDBC Data Sources for a single object store database by using the `configurejdbcos` option.
 - Create the XML file for configuring the LDAP provider by using the `configureldap` option.
 - WebSphere Application Server and JBoss Application Server only. Create the XML file for configuring the login modules by using the `configureloginmodules` option.
1. Log on to the application server as *config_mgr_user*, the user who will run Configuration Manager.
 2. Change the current directory to *ce_install_path/tools/configure*.
 3. Run the appropriate command for the task you need. Do not type any line breaks when you enter the command.

WebSphere Application Server only. Generate the `configurebootstrap.xml` file for the `configurebootstrap` task:

```
configmgr_cl generateconfig -appserver app_server_type
-repositorytype ldap_repository_type
-task configurebootstrap -bootstrap bootstrap_operation
-profile myprofile
```

Generate the `configurejdbcgcd.xml` file for the `configurejdbcgcd` task for the GCD data sources:

```
configmgr_cl generateconfig -appserver app_server_type
-repositorytype ldap_repository_type -db db_type
-task configurejdbcgcd -profile myprofile
```

Generate the `configureldap.xml` file for the `configureldap` task:

```
configmgr_cl generateconfig -appserver app_server_type
-repositorytype ldap_repository_type -ldap ldap_type
-task configureldap -profile myprofile
```

Generate the `configureloginmodules.xml` file for the `configureloginmodules` task:

```
configmgr_cl generateconfig -appserver app_server_type
-repositorytype ldap_repository_type -task configureloginmodules
-profile myprofile
```

where:

-appserver *appserver_name*

-appserver *appserver_type* specifies the type of application server and must be WebSphere.

-repositorytype *ldap_repository_type*

WebSphere Application Server only. The **-repositorytype**

ldap_repository_type parameter specifies the type of LDAP repository to use and must be standalone or federated.

-db *database_type*

The **-db** *database_type* parameter is required only when you are generating files by using the `configurejdbcgcd` or `configurejdbcos` option. This parameter specifies the type of database to be used by Content Platform Engine and must be `mssql`, `oracle`, `oracle_rac`, `db2`, or `db2zos`.

-ldap *ldap_type*

The **-ldap** *ldap_type* parameter is required only when you are generating all the files at the same time or when you are generating a single file by using the `configureldap` option. This parameter specifies the type of directory service repository that Content Platform Engine uses for authenticating users and must be `activedirectory`, `adam`, `ca`, `edirectory`, `oid`, `oracledirectoryse`, or `tivoli`. The `adam` value applies to both Microsoft ADAM and AD LDS.

-bootstrap *bootstrap_operation*

The **-bootstrap** *bootstrap_operation* parameter is required only when you are generating all the files at the same time or when you are generating a single file by using the `configurebootstrap` option. This parameter specifies the bootstrap and text extraction operation for the profile and must be `new`, `modify`, or `upgrade`.

- *myprofile*

The **-profile** *myprofile* parameter specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as `ce_was_tiv_db2`. The profile must be located in the `ce_install_path/tools/configure/profiles` directory, where `ce_install_path` is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2"` or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2`.
- The fully qualified path to the profile input file, such as `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg"` or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg`.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg"`.

4. Repeat as needed to generate all the required XML configuration files.

Creating the data sources by using the command line:

You must create the JDBC data sources for each object store that Content Platform Engine uses. You must generate, edit, and execute a new `configurejdbcos.xml` file for each object store in your environment.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

If you generated all of the configuration profiles at the same time, you have already created an initial `configurejdbcos.xml` file for the initial object store data sources. If you have an existing `configurejdbcos.xml` file, you can generate another file for each additional object store. Each additional file that you add is named `configurejdbcos.n.xml`. You can generate multiple `configurejdbcos.n.xml` files as needed, depending on the number of object stores in your environment. For best results, create an additional file for each object store.

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Configuration Manager values for this task, filter by **CM: Configure Object Store JDBC Data sources (object store 1)** in the **Installation or Configuration Program** column.

2. Log on to the application server as `config_mgr_user`, the user who runs Configuration Manager.
3. If you did not generate all the configuration files at the same time or if you must create another file, generate the `configurejdbcos.n.xml` file by running the following command:

```
configmgr_cl generateConfig -appserver app_server_type -db db_type  
-task configurejdbcos -profile myprofile
```

where:

-appserver *appserver_name*

The **-appserver** *appserver_type* specifies the type of application server and must be WebSphere, WebLogic, or JBoss.

-db *database_type*

The **-db** *database_type* parameter is required only when you are generating all the files at the same time or when you are generating a single file by using the `configurejdbcgcd` or `configurejdbcos` option. This parameter specifies the type of database to be used by Content Platform Engine and must be `mssql`, `oracle`, `oracle_rac`, `db2`, or `db2zos`.

-profile *myprofile*

The **-profile** *myprofile* parameter specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as `ce_was_tiv_db2`. The profile must be located in the `ce_install_path/tools/configure/profiles` directory, where *ce_install_path* is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2"` or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2`.
- The absolute path to the profile input file, such as `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg"` or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg`.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg".

4. Use a text editor to open the `configurejdbcos.n.xml` file and edit it as follows:
 - a. Provide the entries that are required for your environment by using the values in your worksheet.
 - b. Replace each occurrence of `****INSERT VALUE****` with a value appropriate for your site. See the descriptions in the file for more information.
 - c. Verify that the default values for the remaining properties are correct for your site.
 - d. Set the **enabled** attribute value in the **<configuration>** tag to true so that you can run the configuration task in 6.
 - e. Save your edits.
5. Run the **storepasswords** command to encrypt and store the required passwords.

```
configmgr_cl storepasswords -profile myprofile
```
6. Run the following command to execute the `configurejdbc.n.xml` file:

```
configmgr_cl execute -task configurejdbcos -profile myprofile
```

Tip: If the **storepasswords** command prompts you to store passwords in configuration files on disk, you must respond with yes or no (instead of y or n).

7. Optional: Check the completion status by running the following command:

```
configmgr_cl checkStatus -task configurejdbcos -task configurejdbc.n.xml -profile myprofile
```


Where `configurejdbc.n.xml` is the task file for the object store.

8. Repeat step 3 on page 33 through step 6 as needed for each additional object store.

Related concepts:

 [Specifying accounts](#)

For details on accounts and required permissions, see *Plan and Prepare Your Environment for IBM FileNet P8*.

 [Installation and upgrade worksheet](#)

For more information about the installation and upgrade worksheet, see the worksheet topics in *Plan and Prepare Your Environment for IBM FileNet P8*.

Editing the configuration XML files for a Content Platform Engine instance:

You must edit each configuration XML file to provide the property values for your environment. You can use any text editor to open and edit the files.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

If you plan to configure Content Platform Engine to use the directory server's email attribute or, for Active Directory, the userPrincipalName (UPN) to be the user short name that is used for login, then you must perform additional configuration steps and enter specific values for your LDAP and bootstrap settings. For detailed steps, see the FileNet P8 help topic **Security > IBM FileNet P8 security > How to... > Configure Content Engine to use e-mail or UPN for login**.

Note: In high availability environments, make sure to use values appropriate to your configuration:

Database server name

If you are using a highly available database for the global configuration database(GCD), use the virtual server name.

To edit values in the configuration XML files:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Configuration Manager values, in the **Installation or Configuration Program** column filter by one of the following items, depending on which XML file you are editing:

- **CM: Set Application Server properties**
- **CM: Configure GCD JDBC Data Sources**
- **CM: Configure Object Store JDBC Data Sources**
- **CM: Configure LDAP**
- **CM: Configure Bootstrap Properties**

2. Use a text editor or XML editor to open one of the following configuration XML files that you generated:

- applicationserver.xml
- configurejdbcgcd.xml for the global configuration database (GCD)
- configurejdbcos.xml
- configureldap.xml
- configurebootstrap.xml

Do not edit the configureloginmodules.xml, configurejdbcos.xml, or deployapplication.xml files at this time.

3. Make the following changes to each XML configuration file:
 - a. Replace each occurrence of ****INSERT VALUE**** with a value appropriate for your site. See the descriptions in the file for more information.

Important: You do not need to supply values for passwords. You can run the **storepasswords** command later to add encrypted passwords to the file.

- b. Verify that the default values for the remaining properties are correct for your site.
 - c. Set the **enabled** attribute value in the <configuration> tag to true in any configuration XML file you edit if you want to run the configuration task.
4. (WebSphere Application Server only) If you created XA and non-XA data sources that you want to use for the GCD, make the following edits:
 - a. In the configurejdbcgcd.xml file, set the **enabled** attribute value to false in the <configuration> tag to avoid creating another pair (XA and non-XA) of data sources.
 - b. In the configurebootstrap.xml file, set the **<JDBCDataSourceXAFileName>** and **<JDBCDataSourceFileName>** values to the XA and non-XA JNDI names, respectively, that are associated with the GCD.
 5. Save your edits and close the XML file.
 6. Optional: Add encrypted passwords to the XML files by running the **storepasswords** command.

Tip: If the **storepasswords** command prompts you to store passwords in configuration files on disk, you must respond with yes or no (instead of y or n).

- a. Enter the following command on one line:

```
configmgr_cl storepasswords [-task task_type | -taskfile task_file_name]
                             -profile myprofile
```

where:

-task task_type

The **-task task_type** parameter is optional and specifies a task for which to encrypt passwords. The *task_type* value is not case sensitive. The following table lists each valid task name, its associated configuration XML file, and a description of the Content Platform Engine settings affected by the task.

Table 7. *task_type* values

Task	Configuration file	Description
omitted	applicationserver.xml	When you omit the -task task_type parameter, you are prompted to enter the passwords for each configuration XML file in the profile. Each password is encrypted before it is added to the XML file.
	configurebootstrap.xml	
	configurejdbcgcd.xml	
	configurejdbcos.xml	
	configureldap.xml	
	deployapplication.xml	
configurebootstrap	configurebootstrap.xml	Encrypts the password for the BootstrapPassword property, which is used to create the GCD and to start Content Platform Engine.
configurejdbcgcd	configurejdbcgcd.xml	Encrypts the password for the DatabasePassword property, which Content Platform Engine uses to access the GCD.
configurejdbcos	configurejdbcos.xml	Encrypts the password for the DatabasePassword property, which Content Platform Engine uses to access the database that the data source points to.
	configurejdbcos. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	
		If you have more than one configurejdbcos. <i>n</i> .xml file, run the command for each task file.

-taskfile task_file_name

The **-taskfile task_file_name** parameter specifies the configuration XML file to use.

If only one task file exists for the *task_type*, then the **-taskfile task_file_name** parameter is optional.

If more than one task file for the *task_type* exists, then you must include the **-taskfile** *task_file_name* parameter. You can omit the **-task** *task_type* parameter when you specify the **-taskfile** *task_file_name* parameter.

-profile *myprofile*


The **-profile** *myprofile* parameter specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as *ce_was_tiv_db2*. The profile must be located in the *ce_install_path*/tools/configure/profiles directory, where *ce_install_path* is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2" or /opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2.
- The absolute path to the profile input file, such as "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg" or /opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg".

7. Repeat this procedure as needed until you have edited all the required files.

Related concepts:

 Installation and upgrade worksheet

For more information about the installation and upgrade worksheet, see the worksheet topics in *Plan and Prepare Your Environment for IBM FileNet P8*.

Running the configuration XML files:

Running the configuration XML files applies the settings. You use the **execute** command to apply your configuration settings from the command line.

If you need to run the configuration XML files for a profile that was created or edited in the Configuration Manager graphical user interface, verify that the XML files contain values for the required passwords before you attempt to run the files. See "Handling passwords in Configuration Manager" on page 155 for more information.

To run the configuration XML files:

1. Start or stop the application server instance.

Option	Description
WebSphere Application Server	Start the application server instance if it is not already running.

2. Run the configuration XML files, either all at the same time or one file at a time.

"Running all the configuration XML files at the same time" on page 38

From the command line, you can run all of the required configuration XML

files for Content Platform Engine at the same time with a single command. Any configuration XML file that has the enabled element set to false is skipped.

“Running one configuration XML file at a time” on page 39

From the command line, you can run each of the required configuration XML files one file at a time. You must run each of the required files to complete the Content Platform Engine configuration.

Related tasks:

Starting or stopping an application server instance

Running all the configuration XML files at the same time:

From the command line, you can run all of the required configuration XML files for Content Platform Engine at the same time with a single command. Any configuration XML file that has the enabled element set to false is skipped.

If your FileNet P8 domain uses multiple non-managed application servers, then you use a copy of a single EAR file with the bootstrap settings on all the servers. After you run all the tasks on the initial server, you copy the EAR file with the bootstrap settings to the additional servers. Then, when you run the tasks for the additional servers, do not use this procedure to run all tasks at once on the additional servers. Instead, only run the tasks for configuring the JDBC data sources for the GCD, configuring the JDBC data sources for the object stores, and configuring the LDAP provider.

For all other configurations, you can run all the tasks at once on each Content Platform Engine server.

To run all the configuration XML files at the same time:

1. Change the current directory to `ce_install_path/tools/configure`, where `ce_install_path` is the location where the Content Platform Engine software is installed.

2. Run the following command.

```
configmgr_cl execute -profile myprofile
```

where the **-profile** `myprofile` parameter specifies the profile to use. The `myprofile` value can be one of the following items:

- The name of the profile, such as `ce_was_tiv_db2`. The profile must be located in the `ce_install_path/tools/configure/profiles` directory, where `ce_install_path` is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2"` or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2`.
- The absolute path to the profile input file, such as `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg"` or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg`.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg"`.

3. If your FileNet P8 domain uses multiple non-managed application servers, then copy the `ce_install_path/ContentEngine/tools/configure/profiles/my_profile/ear/Engine-app_server_type.ear` file to the Configuration Manager profile directory on each additional Content Platform Engine server.

install_dir

The location where Content Platform Engine is installed.

my_profile

The directory for the Configuration Manager profile that you created.

Engine-app_server_type.ear

The EAR file for your application server type: Engine-ws.ear, Engine-wl.ear, or Engine-jb.ear.

Important: For each additional non-managed server, only run the tasks for configuring the JDBC data sources for the GCD, configuring the JDBC data sources for the object stores, and configuring the LDAP provider.

The task execution status messages are displayed.

Running one configuration XML file at a time:

From the command line, you can run each of the required configuration XML files one file at a time. You must run each of the required files to complete the Content Platform Engine configuration.

If you are running tasks for a profile that was created or edited in the Configuration Manager graphical user interface, verify that the XML files contain values for the required passwords before you attempt to run the configuration XML files. See “Handling passwords in Configuration Manager” on page 155 for more information.

You must run the configuration XML files for each of the required configuration tasks:

- Apply the bootstrap properties file by using the `configurebootstrap` option.
If your FileNet P8 domain uses multiple non-managed application servers, then you use a copy of a single EAR file with the bootstrap settings on all the servers. After you apply the bootstrap properties file on the initial server, you copy the EAR file with the bootstrap settings to the profiles directory on the additional servers. Then, when you run the tasks for the additional servers, do not use the `configurebootstrap` option. Only run the tasks for configuring the JDBC data sources for the global configuration database (GCD), configuring the JDBC data sources for the object stores, and configuring the LDAP provider.
For all other configurations, you can run all the tasks on each Content Platform Engine server.
- Configure the JDBC Data Sources for the GCD by using the `configurejdbcgcd` option.
- Configure the JDBC Data Sources for a single object store database by using the `configurejdbcos` option.
- Configure the LDAP provider by using the `configureldap` option.
- Configure the login modules by using the `configureloginmodules` option.

To run the configuration XML files one file at a time:

1. Change the current directory to `ce_install_path/tools/configure`, where `ce_install_path` is the location where Content Platform Engine is installed.

2. Run the appropriate command for the task you need to complete. Do not type any line breaks when you enter the command.

Run the configurejdbcos.xml file in a profile with one configurejdbcos task:

```
configmgr_cl execute -task configurejdbcos -profile myprofile
```

Run the configurejdbc.2.xml file in a profile with multiple configurejdbcos tasks:

```
configmgr_cl execute -taskfile configurejdbc.2.xml  
-profile myprofile
```

Run the configureldap.xml file in a profile with one configureldap task:

```
configmgr_cl execute -task configureldap -profile myprofile
```

Run the configureldap.3.xml file in a profile with multiple configureldap tasks:

```
configmgr_cl execute -taskfile configureldap.3.xml -profile myprofile
```

Run the configureloginmodules.xml file:

```
configmgr_cl execute -task configureloginmodules -profile myprofile
```

Run the configurebootstrap.xml file in a profile with one configurebootstrap task:

```
configmgr_cl execute -task configurebootstrap -profile myprofile
```

Where:

-taskfile *task_file_name*

The **-taskfile** *task_file_name* parameter specifies the configuration XML file to use.

If only one task file exists for the *task_type*, then the **-taskfile** *task_file_name* parameter is optional, but do not use the **-task** *task_type* parameter with the **-taskfile** *task_file_name* parameter.

If more than one task file for the *task_type* exists, then you must include the **-taskfile** *task_file_name* parameter. You can omit the **-task** *task_type* parameter when you specify the **-taskfile** *task_file_name* parameter.

-profile *myprofile*

The **-profile** *myprofile* parameter specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as *ce_was_tiv_db2*. The profile must be located in the *ce_install_path*/tools/configure/profiles directory, where *ce_install_path* is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2" or /opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2.
- The fully qualified path to the profile input file, such as "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg" or /opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg".

Remember: The values that you entered for the configurejdbcgcd task were for the GCD data sources. You must edit and run the configurejdbcos task once for each object store later in the installation process.

3. If your FileNet P8 domain uses multiple non-managed application servers, then copy the `ce_install_path/ContentEngine/tools/configure/profiles/my_profile/ear/Engine-app_server_type.ear` file to the directory on each additional Content Platform Engine server.

install_dir

The location where Content Platform Engine is installed.

my_profile

The directory for the Configuration Manager profile that you created.

Engine-app_server_type.ear

The EAR file for your application server type: Engine-ws.ear, Engine-wl.ear, or Engine-jb.ear.

Important: For each additional non-managed server, only run the tasks for configuring the JDBC data sources for the GCD, configuring the JDBC data sources for the object stores, and configuring the LDAP provider. When you run the tasks for the additional servers, do not use the configurebootstrap option on the additional servers.

4. Repeat this procedure as needed to run one of the other configuration XML files until you run the files for each of the four required tasks on this server.

The task execution status messages are displayed.

Checking the completion status of Content Platform Engine configuration tasks:

Task execution messages are displayed in the console when you run a task, and you can view the status of a specific task at any time by running the **checkStatus** command. From the command line, you can check the status of all the configuration tasks or check the status of a single task.

The following table lists the status results and their descriptions.

Table 8. checkstatus command results

Status Result	Description
COMPLETED	The task ran successfully.
INCOMPLETE	The task is incomplete.
NO STATUS AVAILABLE	The task has not been run.
FAILED	The task failed to complete. Additional information about the failure is displayed.

“Checking the completion status of all configuration tasks at once”

From the command line you can check the status of all the configuration tasks with a single command. Checking the completion status does not validate the information in the XML files.

“Checking the completion status of one configuration task at a time” on page 42

From the command line you can check the status of a single task.

Checking the completion status of all configuration tasks at once:

From the command line you can check the status of all the configuration tasks with a single command. Checking the completion status does not validate the information in the XML files.

To check the status of a configuration task:

1. Change the current directory to *ce_install_path*/tools/configure, where *ce_install_path* is the location where the Content Platform Engine software is installed.
2. Run the following command:

```
configmgr_cl checkstatus -profile myprofile
```

where the **-profile** *myprofile* parameter specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as *ce_was_tiv_db2*. The profile must be located in the *ce_install_path*/tools/configure/profiles directory, where *ce_install_path* is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2" or /opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2.
- The fully qualified path to the profile input file, such as "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg" or /opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg".

The task execution status messages are displayed.

Checking the completion status of one configuration task at a time:

From the command line you can check the status of a single task.

To check the status of a configuration task:

1. Change the current directory to *ce_install_path*/tools/configure, where *ce_install_path* is the location where the Content Platform Engine software is installed.
2. Run one of the following commands. Do not type any line breaks when you enter the command.

- To check the status of the configurejdbc.xml file in a profile with one configurejdbcos task:

```
configmgr_cl checkstatus -task configurejdbcos -profile myprofile
```

- To check the status of the configurejdbcos.n.xml file in a profile with multiple configurejdbcos tasks:

```
configmgr_cl checkstatus -task configurejdbcos -taskfile task_file_name  
-profile myprofile
```

- To check the status of the configureldap.xml file in a profile with one configureldap task:

```
configmgr_cl checkstatus -task configureldap -profile myprofile
```

- To check the status of the `configureLDAP.n.xml` file in a profile with multiple `configureldap` tasks:

```
configmgr_cl checkstatus -task configureldap -taskfile task_file_name
-profile myprofile
```

- To check the status of the `configureloginmodules.xml` file for the `configureloginmodules` task:

```
configmgr_cl checkstatus -task configureloginmodules -profile myprofile
```

- To check the status of the `configurebootstrap` task:

```
configmgr_cl checkstatus -task configurebootstrap -profile myprofile
```

where:

-taskfile *task_file_name*

The **-taskfile** *task_file_name* parameter specifies the configuration XML file to use.

If only one task file exists for the *task_type*, then the **-taskfile** *task_file_name* parameter is optional, but do not use the **-task** *task_type* parameter with the **-taskfile** *task_file_name* parameter.

If more than one task file for the *task_type* exists, then you must include the **-taskfile** *task_file_name* parameter. You can omit the **-task** *task_type* parameter when you specify the **-taskfile** *task_file_name* parameter.

-profile *myprofile*

The **-profile** *myprofile* parameter specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as `ce_was_tiv_db2`. The profile must be located in the `ce_install_path/tools/configure/profiles` directory, where *ce_install_path* is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as "`C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2`" or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2`.
- The absolute path to the profile input file, such as "`C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg`" or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg`.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter "`C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg`".

3. Repeat the previous step as needed to check status on one of the other configuration XML files.

The task execution status messages are displayed.

Deploying Content Platform Engine instances

Depending on your environment, you can use the Configuration Manager graphical user interface, or the command line, to deploy Content Platform Engine instances.

Perform the procedures in this topic after you have performed the configuration tasks in “Configuring Content Platform Engine” on page 17 on the Content Platform Engine.

Restriction: You must use the command line version of Configuration Manager if any of these conditions are true:

- You need an accessible software version of Configuration Manager for people with disabilities to use.

“Deploying instances by using the graphical user interface”

You can deploy a Content Platform Engine Server instance on the web application server by using the graphical user interface. Deploying makes the Content Platform Engine application available for use.

“Deploying Content Platform Engine by using the Configuration Manager command line” on page 45

From the command line you can deploy the Content Platform Engine application on the application server.

Deploying instances by using the graphical user interface

You can deploy a Content Platform Engine Server instance on the web application server by using the graphical user interface. Deploying makes the Content Platform Engine application available for use.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

Tip: For more information on the properties and values you set in the Configuration Manager, roll your mouse over the property name to view the hover help for the property.

To deploy Content Platform Engine:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Configuration Manager deployment values for this task, filter by **CM: Deploy Application** in the **Installation or Configuration Program** column.

2. Log on to the application server machine as *config_mgr_user*, which is the Configuration Manager user.
3. Start Configuration Manager.

Option	Description
AIX, Solaris, HPUX, HPUXi, Linux, Linux on System z®	Type the following command: <code>ce_install_path/tools/configure/configmgr</code> where <i>ce_install_path</i> is the location where the Content Platform Engine server software is installed

4. Select **File > Open Configuration Profile**.
5. Enter the path to the profile for this Content Platform Engine instance, or click **Browse** to locate the *profilename.cfpg* profile file.
6. Click **OK**.

7. Right-click the **Deploy Application** task in the profile pane (left pane), and select **Edit Selected Task**.
8. Provide the property values for your deployment by using the values in your worksheet.
9. (Application server cluster configurations only) Make sure the following settings are used in a high availability environment using cluster configurations:

Deployment type

Verify that **Deployment type** is set to Cluster.

Application server name

Enter the name of the highly available cluster that you have configured.

This configures the global configuration database (GCD) data sources and security settings at the administrative level so that all cluster nodes have access to this vital configuration information.

10. Select **File > Save**.
11. Enable the task. When the task is disabled, the task name includes the text **(Disabled)**. To enable the task, select **Deploy Application (Disabled)** in the profile pane, and then either right-click and choose **Enable Selected Task** from the context menu, or click the **Enable the Selected Task** icon in the task toolbar.
12. Right-click the **Deploy Application** task in the left pane, and select **Run Task**.

Running the deploy task might take several minutes. The task status messages are displayed in the Console pane below the deploy application properties.

Related concepts:

 [Installation and Upgrade Worksheet](#)

Locate the Installation and Upgrade Worksheet in the IBM FileNet P8 Platform Information Center.

Related tasks:

 [IBM FileNet P8 accounts](#)

See the P8 account information for details on how to specify the required accounts and their permissions in the *Plan and Prepare Your Environment for IBM FileNet P8*.

Starting or stopping an application server instance

Deploying Content Platform Engine by using the Configuration Manager command line

From the command line you can deploy the Content Platform Engine application on the application server.

You must generate the `deployapplication.xml` file, edit the file to provide values for your environment, and then execute the deploy task.

If you are deploying multiple Content Platform Engine instances on the same machine, you must generate, edit, and execute a separate `deployapplication.xml` file for each instance. Store the `deployapplication.xml` file for each instance in a separate profile.

Complete the following tasks:

1. "Generating the `deployapplication.xml` file"
The `deployapplication.xml` file contains settings for deploying the Content Platform Engine application. You must use the **generateConfig** command to create the XML file.
2. "Editing the deployment configuration files" on page 47
You must edit the `applicationserver.xml` and `deployapplication.xml` configuration XML files to provide the property values for your environment. You can use any text editor to open and edit the files.
3. "Running the `deployapplication.xml` file" on page 48
From the command line, you can run the **execute** command on the `deployapplication.xml` configuration XML file to deploy the Content Platform Engine application on the web application server.
4. "Checking the configuration status of the `deployapplication` task" on page 49
From the command line you can check the status of a single task, such as the `deployapplication` task. Checking the completion status does not validate the information in the XML files.

Generating the `deployapplication.xml` file

The `deployapplication.xml` file contains settings for deploying the Content Platform Engine application. You must use the **generateConfig** command to create the XML file.

The `deployapplication.xml` file is created when you generate all files at the same time or when you generate the `deployapplication` task. If you generated all the files at the same time, you already have `deployapplication.xml` file and you can skip this procedure.

To generate the `deployapplication.xml` file:

1. Log on to the application server as *config_mgr_user*, the user who will run Configuration Manager.
2. Change the current directory to *ce_install_path/tools/configure*, where *ce_install_path* is the location where Content Platform Engine is installed.
3. Enter the following command without line breaks to generate the `deployapplication.xml` file:

```
configmgr_cl generateconfig -appserver app_server_type -deploy deploy_type
-task deployapplication -profile myprofile
```

Where:

-appserver *appserver_name*

The **-appserver** *appserver_type* specifies the type of application server and must be WebSphere, WebLogic, or JBoss.

-deploy *deploy_type*

The **-deploy** *deploy_type* parameter is required only when you are generating all the files at the same time or when you are generating a single file by using the `deployapplication` option. This parameter specifies the type of Content Platform Engine deployment. The value must be `standard`, `cluster`, or `netdeploy` (network deployment).

Specify `standard` if you are deploying Content Platform Engine to a stand-alone (that is, a server that is not managed or clustered) WebSphere Application Server, Oracle WebLogic Server, or JBoss Application Server.

Specify `cluster` if you are deploying Content Platform Engine to a WebSphere Application Server, Oracle WebLogic Server, or JBoss Application Server cluster.

Specify `netdeploy` if you are deploying Content Platform Engine to a managed WebSphere Application Server instance. That is, you are using Network Deployment to manage individual servers that are not in a cluster.

-profile *myprofile*

The **-profile** *myprofile* parameter specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as `ce_was_tiv_db2`. The profile must be located in the `ce_install_path/tools/configure/profiles` directory, where `ce_install_path` is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2"` or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2`.
- The absolute path to the profile input file, such as `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg"` or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg`.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg"`.

Editing the deployment configuration files

You must edit the `applicationserver.xml` and `deployapplication.xml` configuration XML files to provide the property values for your environment. You can use any text editor to open and edit the files.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

To edit the values in the configuration XML files:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Configuration Manager values, filter by the task you are editing in the **Installation or Configuration Program** column:

- **CM: Set Application Server properties**
 - **CM: Deploy Application**
2. If you have not already edited the `applicationserver.xml` file in “Configuring Content Platform Engine” on page 17, set the application server property values for your site.
 - a. Use a text editor or XML editor to open the `applicationserver.xml` file.
 - b. Replace each occurrence of `****INSERT VALUE****` with a value appropriate for your site. See the descriptions in the file for more information.
 - c. Verify that the default values for the remaining properties are correct for your site.

(Application server cluster configurations only): Make sure the following settings are used in a high availability environment using cluster configurations:

Deployment type

Verify that **Deployment type** is set to Cluster.

Application server name

Enter the name of the highly available cluster that you have configured.

This configures the GCD data sources and security settings at the administrative level so that all cluster nodes have access to this vital configuration information.

- d. Save your edits.
3. Set the deployment property values for your site.
 - a. Use a text editor or XML editor to open the `applicationserver.xml` file.
 - b. Replace each occurrence of `****INSERT VALUE****` with a value appropriate for your site. See the descriptions in the file for more information.
 - c. Set the **enabled** attribute value in the **<configuration>** tag to true. By default, the **enabled** value is set to false. For deployment to occur, you must enable the task.
 - d. Verify that the default values for the remaining properties are correct for your site.

WebSphere Application Server only:

 - 1) For standard deployment or non-cluster network deployment, specify values for `<applicationservername>` and `<applicationservernode>`.
 - 2) For cluster deployment, specify values for `<applicationservername>`, `<applicationservernode>`, and `<applicationserverclustername>`.
 - e. Save your edits.
4. Run the **storepasswords** command to encrypt and store the web application server administrator password.

```
configmgr_cl storepasswords -profile myprofile
```

Tip: If the **storepasswords** command prompts you to store passwords in configuration files on disk, you must respond with yes or no (instead of y or n).

Related concepts:



Installation and upgrade worksheet

For more information about the installation and upgrade worksheet, see the worksheet topics in *Plan and Prepare Your Environment for IBM FileNet P8*.

Running the deployapplication.xml file

From the command line, you can run the **execute** command on the `deployapplication.xml` configuration XML file to deploy the Content Platform Engine application on the web application server.

To run the `deployapplication.xml` file:

1. Navigate to `ce_install_path/tools/configure`, where `ce_install_path` is the path where you installed Content Platform Engine.
2. Run the following command:

```
configmgr_cl execute -task DeployApplication -profile myprofile
```

where the **-profile** `myprofile` parameter specifies the profile to use. The `myprofile` value can be one of the following items:

- The name of the profile, such as `ce_was_tiv_db2`. The profile must be located in the `ce_install_path/tools/configure/profiles` directory, where `ce_install_path` is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as "`C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2`" or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2`.
- The absolute path to the profile input file, such as "`C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg`" or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg`.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter "`C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg`".

Checking the configuration status of the deployapplication task

From the command line you can check the status of a single task, such as the `deployapplication` task. Checking the completion status does not validate the information in the XML files.

To check the status

1. Set the current directory to `ce_install_path/tools/configure`, where `ce_install_path` is the location where Content Platform Engine is installed.
2. At the command prompt, run the following command:

```
configmgr_cl checkStatus -task deployapplication -profile myprofile
```

where the **-profile** *myprofile* parameter specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as `ce_was_tiv_db2`. The profile must be located in the `ce_install_path/tools/configure/profiles` directory, where `ce_install_path` is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as "`C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2`" or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2`.
- The absolute path to the profile input file, such as "`C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg`" or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg`.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter "`C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg`".

The task execution status messages are displayed.

Installing storage device source files

If your FileNet P8 system includes Tivoli Storage Manager or EMC Centera devices, you must install files on the Content Platform Engine server.

“Installing Tivoli Storage Manager client and adding native API library paths (WebSphere Application Server)”

The client software and the native API library paths enable you to use Tivoli Storage Manager to access a fixed content device.

“Installing or updating EMC Centera SDK library files” on page 51
EMC Centera SDK library files enable access between the FileNet P8 environment and EMC Centera fixed content devices. You need to update the EMC Centera SDK library files if EMC Centera fixed content devices are in your existing environment or if EMC Centera fixed content devices will be added to your FileNet P8 environment.

Installing Tivoli Storage Manager client and adding native API library paths (WebSphere Application Server)

The client software and the native API library paths enable you to use Tivoli Storage Manager to access a fixed content device.

“Installing Tivoli Storage Manager client”

Install the Tivoli Storage Manager client software on each application server where Content Platform Engine is deployed.

“Copying the Tivoli Storage Manager API libraries to additional servers”

If you are running a Content Platform Engine server farm, the Tivoli Storage Manager API libraries must be on each server in the farm.

“Creating a shared library definition for Tivoli Storage Manager native API library files” on page 51

The shared library definition specifies the location of the Tivoli Storage Manager JAR file.

Installing Tivoli Storage Manager client

Install the Tivoli Storage Manager client software on each application server where Content Platform Engine is deployed.

To install Tivoli Storage Manager client software:

1. Download the Tivoli Storage Manager client software from the IBM Support site at <http://www.ibm.com/support/docview.wss?uid=swg24019757>.
2. Complete the platform-specific installation instructions included with each Tivoli Storage Manager client download package. Record the path where you install Tivoli Storage Manager client because you must specify the path as the DSMI directory when you create a Tivoli Storage Manager fixed content device in FileNet Enterprise Manager. If you are installing Tivoli Storage Manager client on multiple AIX, Solaris, HP-UX, HP-UXi, Linux, or Linux for System z hosts, the installation path must be the same on each host.

Copying the Tivoli Storage Manager API libraries to additional servers

If you are running a Content Platform Engine server farm, the Tivoli Storage Manager API libraries must be on each server in the farm.

To copy the Tivoli Storage Manager API libraries to additional servers:

Copy the entire tsm100 directory structure from the Content Platform Engine installation directory to each of the servers in the farm. It is a best practice to use the same directory structure on each server in the farm. For example:

Option	Description
AIX, Solaris, HPUNIX, HPUNIXi, Linux, Linux for System z	/opt/IBM/FileNet/ContentEngine/tsm100

Creating a shared library definition for Tivoli Storage Manager native API library files

The shared library definition specifies the location of the Tivoli Storage Manager JAR file.

To create a shared library definition for Tivoli Storage Manager native API library files:

1. Log on to the WebSphere administrative console.
2. Create a shared library definition according to the type of deployment (stand-alone or clustered), the version of WebSphere, and the operating system on which WebSphere runs, as shown in the following substeps.
 - a. Specify a Node scope for the library.
 - b. In a server farm, if you installed the tsm100 directory in different locations, choose Server scope and add a Shared Library entry for each server in your server farm.
 - c. Provide a name for the shared library, for example TSMAPLIB.
3. Navigate to the deployed FileNetEngine application and then set the created shared library reference.
4. Save the change to the master configuration.

Related information:

WebSphere Application Server Library

Installing or updating EMC Centera SDK library files

EMC Centera SDK library files enable access between the FileNet P8 environment and EMC Centera fixed content devices. You need to update the EMC Centera SDK library files if EMC Centera fixed content devices are in your existing environment or if EMC Centera fixed content devices will be added to your FileNet P8 environment.

“Installing EMC Centera SDK library files”

EMC Centera SDK library files enable communication between the FileNet P8 environment and the EMC Centera fixed content devices.

“Configuring EMC Centera SDK environment variables” on page 52

You must specify values for the environment variables so that Content Platform Engine can access the EMC Centera SDK library files.

Installing EMC Centera SDK library files

EMC Centera SDK library files enable communication between the FileNet P8 environment and the EMC Centera fixed content devices.

To install EMC Centera SDK library files:

1. Log on to the Content Platform Engine Server machine as *cpe_install_user*.
2. Back up or delete any existing EMC Centera SDK library files, which, by default, are located in the Default Destination Installation Location indicated in the following table:

Table 9. Destination installation location

Operating System	Default Destination Installation Location
Linux,, Linux for System z	/usr/local/Centera_SDK

3. The Centera directory in the Content Platform Engine software package contains the EMC Centera SDK installation files. As shown in the following table, copy the appropriate directory to a location on the Content Platform Engine Server machine, such as /tmp (AIX, Solaris, HPUX, HPUXi, Linux, or Linux for System z) or C:\Temp (Windows).

Table 10. Directory to be copied

Operating System	Directory To Be Copied
Linux, Linux for System z	Depending on your version of gcc, copy one of the following directories: Centera/gcc3.3 Centera/gcc4

4. On the Content Platform Engine Server machine, navigate within the Centera directory (at its copied location) to the install subdirectory, which contains the installer script.
5. Run the installer script corresponding to the operating system on the Content Platform Engine Server machine. On Windows, specify the install directory, such as C:\Centera_SDK , on the command line. On all other operating systems, the installer script will prompt you for the install directory.

Table 11. Installer script

Operating System	Script
AIX, Solaris, HPUX, HPUXi, Linux, Linux for System z	install.sh

6. The installer script creates 64-bit library directories, and puts them in a default installation directory, depending on your operating system (as shown in the following table). Accept or change the default when prompted by the script.

Table 12. 64-bit library directory default installation directories

Operating System	Subdirectories of extracted EMC Centera SDK	
	Directory	Description
Linux, Linux for System z	../gcc3.3/lib	
	../gcc4/lib	

Configuring EMC Centera SDK environment variables

You must specify values for the environment variables so that Content Platform Engine can access the EMC Centera SDK library files.

To configure EMC Centera SDK environment variables:

1. Locate the sample setup script on the Content Platform Engine installation media. The file name of the sample setup script depends on your operating system:

Option	Description
AIX, Solaris, HPUX, HPUXi, Linux, Linux on System z	setCenteraLibPath.sh

2. Modify the sample setup script as indicated in the following table:

Note that the `CENTERA_LIB_PATH` variable needs to point to the library directory, not just the installation directory that contains the library directory. For example, if you have a 64-bit AIX system, and you change the destination installation path (*install_path* in the table below) from:

`/usr/local/Centera_SDK` (the default)

to:

`/usr/local/Centera/SDKvN.N.NNN`

then change the installation path of the AIX script to:

`/usr/local/Centera/SDKvN.N.NNN/lib/64`

Note that the actual location is appended with either `lib/32` or `lib/64` because the installation script creates both 32-bit and 64-bit library directories, and places them inside the `lib` directory.

Table 13. Script revisions

Operating System	Script Revisions
Linux, Linux for System z	<p>From:</p> <pre>CENTERA_LIB_PATH=/usr/local/Centera_SDK/lib/32 LD_LIBRARY_PATH=\$LD_LIBRARY_PATH: \$CENTERA_LIB_PATH export LD_LIBRARY_PATH</pre> <p>to:</p> <pre>CENTERA_LIB_PATH=install_path /lib/32 LD_LIBRARY_PATH=\$LD_LIBRARY_PATH: \$CENTERA_LIB_PATH export LD_LIBRARY_PATH</pre> <p>or:</p> <pre>CENTERA_LIB_PATH=install_path /lib/64 LD_LIBRARY_PATH=\$LD_LIBRARY_PATH: \$CENTERA_LIB_PATH export LD_LIBRARY_PATH</pre>

3. Copy the modified script text into one of the application server startup scripts shown in the following table, or save the updated script and call it from the application server startup script.

Table 14. Startup scripts

Application Server	Startup Script (AIX, HPUX, Linux, Linux for System z, Solaris)	Startup Script (Windows)
WebSphere Application Server	setupCmdLine.sh	setupCmdLine.cmd

4. Stop and start the application server instance.

Related tasks:

Starting or stopping an application server instance

Configuring file stores for high availability

File store content is managed from the Content Platform Engine application.

Ensure that the file store data is highly available and that access to content in file stores is not interrupted.

All file stores

File systems that are used for file stores must be shared or mounted through the NFS or CIFS protocol.

Each Content Platform Engine instance in a farm must have access to the same shares or mount points.

Standard file stores

Standard file stores must be installed in file systems that are highly available.

Fixed File Stores

The front end of the file system must be made highly available, as indicated previously, and the remote device must be made highly available by using its built-in capability. See your fixed file store documentation for details.

Tip:

- A fixed file store comprises a file system-based front-end, similar to a standard file store, and a remote storage system such as Centera or NetApp/IBM N-Series SnapLock.
- The method and technology used to make file store data highly available can vary greatly, from file servers built on general-purpose hardware and cluster technology, such as IBM HACMP™, to specialized devices with built-in high availability such as NAS- and SAN-based offerings from EMC, NetApp or IBM.
- The implementation and use of these technologies vary, but they can all be used to provide highly available access to data so long as they meet the criteria discussed in this section.

Completing Content Platform Engine post-deployment steps

You must complete the post-deployment web application server configuration before you can put a FileNet P8 system into production.

“Completing Content Platform Engine post-deployment steps (WebSphere)”
You must complete the post-deployment web application server configuration before you can put a FileNet P8 system into production.

Completing Content Platform Engine post-deployment steps (WebSphere)

You must complete the post-deployment web application server configuration before you can put a FileNet P8 system into production.

To complete the post-deployment configuration:

1. Log in to the WebSphere Application Server administrative console.
2. Navigate to **Security > Global security**.

3. If you configured Content Platform Engine to use federated user repositories, complete the following substeps:
 - a. Click **Configure**.
 - b. Specify a unique user for the **Primary administrative user name**. Use the short name. The user name must exist in one of the realms and must be unique.
 - c. Specify the **Server user identity**. You can select **Automatically generated server identity** or specify a name that exists in one of the repositories. The user name must be unique.
 - d. Save your changes to the master configuration.
4. Configure security settings:

Important: Enabling the security settings must be done manually. Deploying Content Platform Engine does not enable or check these settings.

- a. Enable WebSphere administrative security to secure the WebSphere administration console.
 - b. Disable Java 2 security. Otherwise, Content Platform Engine cannot start or process requests.
5. Complete the following substeps to verify that the HTTP port used by the Content Platform Engine is defined in the default_host host aliases table. By default the host alias is defined only for HTTP port 9080. If you are using any other HTTP port (common in network deployments) you must add that port to the list of host aliases for default_host.
 - a. Navigate to **Environment > Virtual Hosts > default host > Host Aliases**.
 - b. Add your HTTP port in the host aliases table.
 - c. Click **OK**, and then click **Save**.
 6. Restart the WebSphere application server instance where Content Platform Engine is deployed, as shown in the following table. .

Option	Description
Stand-alone server	Stop and start the application server instance.
Network Deployment	Stop and start the application server instance where Content Platform Engine is deployed, including the Deployment Manager and all managed nodes.
Cluster	Stop and start the cluster, as well as the deployment manager and all of its managed nodes.

Related tasks:

Starting or stopping an application server instance

Verifying the Content Platform Engine deployment

You can verify that the Content Platform Engine deployment was successful by accessing the FileNet P8 System Health page.

In a highly available environment, verify that the Content Platform Engine application is running on the cluster or farm.

To verify the Content Platform Engine deployment:

1. Browse to the FileNet P8 System Health page:

`http://server:port/P8CE/Health`

where:

server is the host name of the machine where Content Platform Engine is deployed.

port is the WSI port used by the Web application server on the machine where Content Platform Engine is deployed.

In a highly available environment, use the load balanced virtual name for the *server:port*. For example: `http://virtual_server/P8CE/Health`.

The following table lists an example address for your application server:

Table 15. Example FileNet P8 System Health page address

Application Server Type	Web Page Address
IBM WebSphere Application Server	<code>http://server:9080/P8CE/Health</code>

2. Verify that the FileNet P8 System Health page contains the Content Platform Engine instance host name and port number. The FileNet P8 System Health page provides status for the items in the following table.

Tip: At this point, red icons appear on the page at the left of those entries that do not yet exist.

Table 16. FileNet P8 System Health page contents

Section	Description
Domain	Displays the FileNet P8 domain name if a domain was found.
Global Configuration Database	Verifies that the GCD contains a valid domain object, that the XA and non-XA data sources are defined and have unique names, and that the bootstrap user name and password are defined. If any of these verification tests fail, then the failed icon is displayed.
Directory Configurations	Verifies that at least one directory service is configured and lists the number of configured directory service providers.
PE Connection Points	Displays the number of Process Engine connection points.
PE Isolated Regions	Displays the number of Process Engine isolated regions.
Fixed Content Devices	Lists the number of fixed content devices (FCDs) For each FCD listed, there is at least one associated fixed storage area that is in the open state.
Object Stores	Verifies that at least one object store exists and lists the number of object stores.
Storage Areas	Verifies that at least one storage area is defined, lists the number of storage areas, and the status for each storage area, such as online or offline.
Content Cache Areas	Displays the number of content cache areas.
Sites	Verifies that at least one site is defined and lists the number of sites. For each site listed, at least one virtual server or server instance exists.

3. Optional: Bookmark the FileNet P8 System Health page Web page address in your browser for later use.
4. Browse to the Content Platform Engine Startup Context (Ping Page):

`http://server:port/FileNet/Engine`

where:

server is the host name of the machine where Content Platform Engine is deployed.

port is the HTTP port used by the application server where Content Platform Engine is deployed.

In a highly available environment, use the load balanced virtual name for the *server:port* . For example: `http://virtual_server/FileNet/Engine`.

The following table lists an example address for your application server:

Table 17. Example Content Platform Engine Startup Context (Ping Page) address

Application Server Type	Web Page Address
IBM WebSphere Application Server	<code>http://myserver:9080/FileNet/Engine</code>

5. Verify that the Content Platform Engine Startup Context (Ping Page) contains the following information:
 - Verify the value in the **Startup Message** key. The Content Platform Engine build and version (for example, dap511.097), must match the build and version in the *ce_install_path/ce_version.txt* file, where *ce_install_path* is the location where the Content Platform Engine software is installed.
 - Verify that the values for JDBC driver, server instance, operating system, and other properties match the values that you entered when you configured Content Platform Engine.
6. Optional: Bookmark the Content Platform Engine Startup Context (Ping Page) in your browser for later use.
7. (Highly available environments): View the startup context name of the load-balancer or proxy device to verify the functionality of the load-balanced environment, or the name of the physical server to verify a single server.
8. (Highly available environments): Verify Content Platform Engine access through the load balancer.
 - a. Browse to:
`http://ce_load_balancer:port/FileNet/Engine`

where *ce_load_balancer* is name of the load-balancer or proxy device to verify the functionality of the load balanced environment and *port* is the port used to access Content Platform Engine on the load balancer or server running Content Platform Engine.
 - b. Load the Content Platform Engine Startup Context page and verify that Content Platform Engine is accessed correctly by using the load balancer.
 - c. View the startup context.name of the load-balancer or proxy device to verify the functionality of the load-balanced environment, or the name of the physical server to verify a single server.

Tip:

- Depending on your configuration you can connect to the load balanced Content Platform Engine installation, and after confirming that Content Platform Engine is up and running, you can refresh your browser to have the load balancer cycle through all managed nodes for verification.

Related tasks:

Starting or stopping an application server instance

Creating the FileNet P8 domain

You need to create a FileNet P8 domain to contain the object stores, storage areas, index areas, and other entities that you create.

Create only one FileNet P8 domain per highly available environment.

To create a FileNet P8 domain:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled, and filter by **ACCE: Create FileNet P8 domain** in the **Installation or Configuration Program** column.

2. Start IBM Administration Console for Content Platform Engine if you did not already do so. The Create a New Domain wizard starts automatically the first time IBM Administration Console for Content Platform Engine runs.
 - a. On any computer, open a browser and navigate to `http://CPE_Server:port/acce`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.
 - b. Log on as the *gcd_admin* user.
3. Complete the wizard by using the values in your worksheet. The values that are displayed in the wizard screens are default values, which you must change to match your site.

Creating a database connection

You must create a database connection so that Content Platform Engine can connect to the database that is used by object stores and isolated regions.

To create a database connection:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled, and filter by **ACCE: Create a Database Connection** in the **Installation or Configuration Program** column.

2. Start IBM Administration Console for Content Platform Engine if you did not already do so:
 - a. On any computer, open a browser and navigate to `http://CPE_Server:port/acce`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.
 - b. Log on as the *gcd_admin* user.
3. In the navigation pane of IBM Administration Console for Content Platform Engine, expand your FileNet P8 domain. Within the domain, expand the folders **Global Configuration > Administration > Database Connections**. Right-click **Database Connections** and choose **New Database Connection** to start the New Database Connection wizard.

4. Complete the wizard by using the values in your worksheet. The values that are displayed in the wizard screens are default values, which you must change to match your site.

Creating the initial object store

Object stores are used to store documents, workflows and other objects. The New Object Store wizard leads you through the steps required to create an object store.

The New Object Store wizard fails to complete if you try to assign the new object store to a database connection and schema name that has already been used.

If you encounter timeout errors when you create an object store or when you subsequently import add-on features, the transaction timeout value setting might be too low. To modify the transaction timeout value, see the appropriate topic for your application server:

- Specifying the WebSphere environment variables
- Configuring WebLogic Server for Content Platform Engine
- Configuring JBoss Application Server for Content Platform Engine


To create the initial object store:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only IBM Administration Console for Content Platform Engine values for this task, filter by **ACCE: Create Object Store** in the **Installation or Configuration Program** column.

2. Start IBM Administration Console for Content Platform Engine if you did not already do so:
 - a. On any computer, open a browser and navigate to `http://CPE_Server:port/acce`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.
 - b. Log on as the *gcd_admin* user.
3. In the tree view, right-click the **Object Stores** container and choose **New Object Store** to start the wizard.
4. Complete the wizard screens by using the values in your worksheet.

Related concepts:

 Installation and upgrade worksheet

For more information about the installation and upgrade worksheet, see the worksheet topics in *Plan and Prepare Your Environment for IBM FileNet P8*.

Related tasks:

 Storage areas for object stores

For more information about object stores, see *Plan and Prepare Your Environment for IBM FileNet P8*.

Creating a workflow system

You must create a workflow system to contain your isolated regions. When you create a workflow system, you define an isolated region and its connection point. In addition, you can optionally customize the database storage parameters and configure email notification.

Before you create the workflow system, make sure you have gathered the following information:

- Determine the name of the workflow system data table space and optionally the index and BLOB table spaces.
- Determine the security groups that will be granted administrative and configuration privileges for the workflow system.

You must log on to the administration console as a *gcd_admin* user to perform this task.

To create a workflow system:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled, and filter by **ACCE: Create a Workflow System** in the **Installation or Configuration Program** column.

2. Start the New Workflow System wizard in the administration console.
 - a. In the domain navigation pane, select the object store.
 - b. In the object store navigation pane, right-click the **Administrative > Workflow System** folder and click **New** to start the wizard.
3. Complete the wizard steps by using the values in your worksheet. The values that are displayed in the wizard screens are default values, which you must change to match your site.

Connecting to a highly available Content Platform Engine

The configuration of the Content Platform Engine connection in a highly available environment depends on the type of application you want to connect to the Content Platform Engine. You can configure administrative applications or user applications to connect to Content Platform Engine.

Administrative applications, IBM FileNet Deployment Manager, modify metadata and global configuration database information such as property templates, class and property definitions, and domain level objects such as sites, object stores, and file storage areas.

Due to the built-in lag in metadata synchronization across the Content Platform Engine nodes, changes made on one node are not synchronized immediately after a configuration change is made via an administrative application.

In the event the configured Content Platform Engine fails you must reconfigure your administrative applications to point to a different Content Platform Engine node. For information, go to the FileNet P8 online help and navigate to **Administering IBM FileNet P8 > Administering Content Platform Engine > Defining the FileNet P8 infrastructure > FileNet P8 domains > Logging on to a domain**.

User applications such as Workplace and Workplace XT are content- and process-centric applications used in everyday production to check documents in and out and access workflows, for example.

For user applications, the Content Platform Engine connection in a highly available environment differs depending on your HA configuration, but in any case must be

configured to connect to the virtual server, so that it will be redirected automatically to another Content Platform Engine node in the event of a Content Platform Engine node failure.

- If a Java application server cluster is used, EJB connections must use a specific format for establishing connections to Content Platform Engine.
- Applications that use the Web service (CEWS) protocol to connect to Content Platform Engine must use the virtual server name of the hardware or software that is load balancing the connection.

“Content Platform Engine in an application server cluster by using EJB transport”

You can configure clients, such as Application Engine, that use EJB transport to communicate with the Content Platform Engine in an application server cluster.

“Connecting by using Content Engine Web Service Transport (CEWS)” on page 62

You can use load balancers to manage requests to Content Platform Engine in a highly available configuration by connecting the client application to Content Platform Engine using the Web Services (CEWS, previously seen as WSI) transport.

Content Platform Engine in an application server cluster by using EJB transport

You can configure clients, such as Application Engine, that use EJB transport to communicate with the Content Platform Engine in an application server cluster.

For clients such as Application Engine that use an EJB transport to communicate with Content Platform Engine in an application server cluster configuration, you must use an URL with a format different from non-highly available configurations.

Restriction: In these examples, the “cemp” portion at the beginning of the URI is required by FileNet P8 applications, such as Workplace and Workplace XT. If you are developing and using your own applications, the “cemp” prefix is not required.

When Content Platform Engine is made highly available through an application server cluster configuration the Content Platform Engine URL should have the following form (with no carriage returns):

WebSphere Application Server

```
cemp:corbaloc::node1_hostname:BOOTSTRAP_ADDRESS,  
:node2_hostname:BOOTSTRAP_ADDRESS/cell/clusters/  
your_websphere_cluster_name/FileNet/Engine
```

This configuration requires the WebSphere cluster name in addition to the node names as part of the URL. The bootstrap port for a cluster configuration (by default, port 9810) is usually different from the bootstrap port on a non-cluster (standalone) configuration (by default, port 2809).

Only one URL is used regardless of SSL use. WebSphere EJB over SSL is automatically established if EJB security is enabled.

Example:

```
cemp:corbaloc::testnode1:9810,:testnode2:9810/cell/clusters/  
testwascluster/FileNet/Engine
```


If the EJB client is deployed into the same WebSphere Network Deployment cell as Content Platform Engine, you can use the following, simpler corbaloc URL:
`comp:corbaloc:rir:/cell/clusters/your_websphere_cluster_name/FileNet/Engine`

Connecting by using Content Engine Web Service Transport (CEWS)

You can use load balancers to manage requests to Content Platform Engine in a highly available configuration by connecting the client application to Content Platform Engine using the Web Services (CEWS, previously seen as WSI) transport.

Applications such as IBM Content Collector use the Content Engine Web Service (CEWS) transport to connect to Content Platform Engine. CEWS can use load balancers to balance requests to Content Platform Engine servers in a highly available configuration. In this type of configuration clients access Content Platform Engine by using a virtual server name rather than a server name and port number.

Use the load balanced virtual name when configuring a connection to Content Platform Engine to ensure that applications will function in the event of a Content Platform Engine failure.

Use the following format for the Content Platform Engine URL:

`http://virtualname/wsi/FNCEWS40MTOM/`

Example:

`http://testvirtual1/wsi/FNCEWS40MTOM/`

Verifying the Content Platform Engine system

You can verify the Content Platform Engine system by using Administration Console for Content Platform Engine to create a folder in each object store.

To perform this system test, you must have installed Content Platform Engine and have created at least one object store.

If you can complete the steps in this verification test, you will verify that Content Platform Engine is successfully installed, including the following configurations:

- Content Platform Engine is successfully using the *cpe_service_user* account to communicate with the configured directory server.
- Content Platform Engine is successfully using the *cpe_db_user* account to communicate with configured database.

To verify the Content Platform Engine system:

1. Start IBM Administration Console for Content Platform Engine if you did not already do so:
 - a. On any computer, open a browser and navigate to `http://CPE_Server:port/acce`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.
 - b. Log on as the *object_store_admin* user.
2. Start the New Sub Folder wizard in the administration console:
 - a. In the domain navigation pane, select the object store.
 - b. Select the **Browse > Root Folder** folder.

- c. Right-click the **Root Folder** and choose **New Sub Folder** to start the New Sub Folder wizard.
3. Complete the wizard.
4. Optional: Delete the folder object that you just created.
5. In high availability environments, verify failover for all nodes in your configuration.
 - a. Browse to the Content Platform Engine Startup Context page:
`http://ce_server:port/FileNet/Engine`
 - b. Fail one of the Content Platform Engine nodes.
 - c. Verify that you can reload the Startup Context page, and that you can access your object stores by using Administration Console for Content Platform Engine.
 - d. Restart all nodes that you failed during this test.

If you were able to complete these steps, then Content Platform Engine is working properly. If you were not able to complete these steps, see .

Installing and configuring IBM Content Search Services

You can install and configure IBM Content Search Services for a single server configuration or a multiple server configuration on Windows, AIX, Linux, and Solaris operating systems.

IBM FileNet Content Engine preprocesses documents and sends them to the IBM Content Search Services index server for indexing. Depending on the size and configuration of your system, you might want to have multiple server instances of IBM Content Search Services installed on your system.

In a single server configuration, a single instance of the IBM Content Search Services server performs both the indexing and searching tasks for the Content Engine.

In a multiple server configuration, you assign different roles to your IBM Content Search Services server instances to distribute the load for both indexing and searching tasks. You can run multiple server instances of IBM Content Search Services on the same computer for vertical scaling or you can run them on different computers for horizontal scaling. Each server instance of IBM Content Search Services can be designated to do only indexing tasks, searching tasks, or both. You designate which tasks each IBM Content Search Services server does by assigning it a specific server mode:

Index Content Engine sends only indexing tasks to servers in this mode. You can have multiple, dedicated index servers to distribute the indexing load for high volume scenarios. Multiple index servers also allow failover capability for the Content Engine. If one indexing server goes offline, the Content Engine automatically distributes the indexing load to the remaining indexing servers.

Search

Content Engine sends only searching tasks to servers in this mode. You can have multiple, dedicated search servers to distribute the searching load when you have many indexes to search. Multiple search servers also allow failover capability for the Content Engine. If one search server goes offline, the Content Engine automatically selects an alternate search server to perform its tasks.

IndexAndSearch

Content Engine sends both indexing and searching tasks to servers in this mode. The IndexAndSearch server mode is typically used in a single server configuration.

Tip: When considering how to balance available CSS servers, it is important to take into consideration the expected indexing and search scenario. The following table presents possible scenarios and the suggested server mode assignments. Note that even a heavy search load is generally lighter compared to the indexing/ingestion load.

Table 18. Choosing the server mode

Expected scenario	Suggested server mode
A heavy indexing load (for example, an indexing rate of two million documents per day)	Configure more CSS servers in Index mode.
A heavy search load	Configure one or more servers in Search mode. If you are limited to two or three servers, configure one server in Search mode and the other servers in Index mode or IndexAndSearch mode.
A heavy indexing load and a light search load, and you are limited to two or three servers	Configure all CSS servers in IndexAndSearch mode.

Set up the site to contain the object store and the IBM Content Search Services servers. All of the documents and other objects are indexed in the same site as the object store.

“Installing IBM Content Search Services”

You can install IBM Content Search Services either interactively or silently by using the information about the Installation and Upgrade Worksheet that was completed during your planning activities.

“Configuring IBM Content Search Services” on page 69

You must configure IBM Content Search Services to run on Content Platform Engine to manage your indexing and searching tasks.

Installing IBM Content Search Services

You can install IBM Content Search Services either interactively or silently by using the information about the Installation and Upgrade Worksheet that was completed during your planning activities.

The vendor software that is used to install IBM Content Search Services does not support the use of extended (non-English) characters in the installation path. You must use only English characters (not extended characters) in the installation path for IBM Content Search Services.

After you successfully install IBM Content Search Services, you must configure the IBM Content Search Services software to run as an IBM Search server on Content Platform Engine. See *“Installing Content Platform Engine and IBM Case Foundation”* on page 10 for more information.

“Installing IBM Content Search Services interactively” on page 67

You can install IBM Content Search Services interactively by running the installation program. In a multiple-server configuration, run the installation program for each server you want to install.

“Installing IBM Content Search Services silently” on page 67

You can install IBM Content Search Services silently by entering installation values into an input response file and running the installation program from a command line.

“Starting or stopping IBM Content Search Services servers” on page 68

You can manually start or stop the IBM Content Search Services servers that Content Platform Engine uses to index and search for content, by running the startup and shutdown commands for your operating system.

Installing IBM Content Search Services interactively

You can install IBM Content Search Services interactively by running the installation program. In a multiple-server configuration, run the installation program for each server you want to install.

Be sure that you have the Installation and Upgrade Worksheet that was completed during your planning activities.

To install IBM Content Search Services interactively:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only IBM Content Search Services values, filter by **CSS Installer** in the **Installation or Configuration Program** column.

2. Log in to the host computer as the `css_install_user`.
3. Access the IBM Content Search Services installation package and run the installation program.

Table 19. Interactive installation commands

Platform	Command
Linux 32 bit	5.2.0-CSS-LINUX32.BIN
Linux 64 bit	5.2.0-CSS-LINUX64.BIN
Linux for System z	5.2.0-CSS-ZLINUX.BIN

4. Complete the installation program screens by using the values in your Installation and Upgrade Worksheet.

Attention: Make a note of the authentication token that is generated by the installation program. You will specify the token when you configure the IBM Content Search Services server in Administration Console for Content Platform Engine. You can also get the authentication token at a later time by running the IBM Content Search Services configuration tool.

5. Review the `css_install_path/css_install_5.2.0.log` file for installation errors. It is a best practice to review log files even if the IBM Content Search Services installation program does not generate any errors. Some errors noted in the log files are benign. If an error is not benign (that is, you cannot then index or search for documents), see the log file for help in determining the cause.
6. After the installation completes, verify the IBM Content Search Services service is installed and has started.
7. For high availability configuration, repeat this procedure for every server on which want to install IBM Content Search Services.

Important:

If you select the New Server option when you add an IBM Content Search Services server, you do not have to specify the port and server name for the new server. The installation program uses a unique port and server name for the new server.

Installing IBM Content Search Services silently

You can install IBM Content Search Services silently by entering installation values into an input response file and running the installation program from a command line.

Be sure that you have the Installation and Upgrade Worksheet that was completed during your planning activities.

To install IBM Content Search Services silently:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: Tip: In the worksheet file, verify that the **Data > ->Filter > ->AutoFilter** command is enabled. To view only Content Search Engine values, filter by **CSS Installer** in the **Installation or Configuration Program** column.

2. Log on to the host computer as *css_install_user*.
3. Edit the *css_silent_install.txt* file to reflect the appropriate responses for your installation.
4. Save the edited response file to your temporary directory.
5. Go to the temporary directory on your local disk.
6. Run the IBM Content Search Services installation program by running the appropriate command:

Table 20. Silent installation commands

Platform	Command
Linux 32 bit	5.2.0-CSS-LINUX32.BIN -i silent -f css_silent_install.txt
Linux 64 bit	5.2.0-CSS-LINUX64.BIN -i silent -f css_silent_install.txt
Linux for System z	5.2.0-CSS-ZLINUX.BIN -i silent -f css_silent_install.txt

7. Review the *css_install_path/css_install_5.2.0.log* log file for installation errors.

It is a best practice to review log files even if the IBM Content Search Services installation program does not generate any errors. Some errors noted in the log files are benign. If an error is not benign (that is, you cannot then index or search for documents), see the log file for help in determining the cause.

8. After the installation completes, verify the IBM Content Search Services service is installed and has started.
9. For high availability configuration, repeat this procedure for every server that you want to install.

Important:

You must use a different server name and port for each additional server. If you use the same server name and port as a previously installed server, the new server installation overwrites the existing server.

Starting or stopping IBM Content Search Services servers

You can manually start or stop the IBM Content Search Services servers that Content Platform Engine uses to index and search for content, by running the startup and shutdown commands for your operating system.

The default directory location from which you must run these commands is:

- AIX, Linux, Solaris: */opt/IBM/Content_Search_Services/CSS_Server/bin*
- Windows: *C:\Program Files\IBM\Content Search Services\CSS_Server\bin*

Tip: If you installed IBM Content Search Services on Windows as a service, you can start and stop the server by using the Windows service. Go to **Start > Control Panel > Administrative Tools > Services**, right-click on the service, and select the task to run.

To manually start or stop IBM Content Search Services servers:

1. Log in to the computer where the IBM Content Search Services servers are installed as the *css_os_user*.
2. Run one of the following commands, depending on your operating system:

Option	Description
AIX, Linux, Solaris (all supported versions)	Start services: <i>css_install_location/server_name/bin/startup.sh</i> Stop services: <i>css_install_location/server_name/bin/shutdown.sh</i>

Configuring IBM Content Search Services

You must configure IBM Content Search Services to run on Content Platform Engine to manage your indexing and searching tasks.

You can also configure IBM Content Search Services to communicate with Content Platform Engine over a secure connection by using the Secure Sockets Layer protocol.

“Getting the IBM Content Search Services authentication token”

The IBM Content Search Services server uses the authentication token as a security device to identify itself as authorized to communicate with Content Engine. The authentication token is displayed on the last window of the IBM Content Search Services installation program for each server that you install.

“Configuring Content Platform Engine for IBM Content Search Services” on page 70

You must configure IBM Content Search Services as an IBM Content Search Services server on Content Platform Engine.

“Verifying the IBM Content Search Services installation” on page 75

You can verify that the IBM Content Search Services installation was successful by using IBM Administration Console for Content Platform Engine to create a search index job and checking to see whether the job returns the correct index objects.

“Configuring SSL for IBM Content Search Services” on page 76

IBM Content Search Services can communicate with Content Engine on both secure and nonsecure channels. You can configure IBM Content Search Services to communicate over a secure connection by using the Secure Sockets Layer (SSL) protocol.

Getting the IBM Content Search Services authentication token

The IBM Content Search Services server uses the authentication token as a security device to identify itself as authorized to communicate with Content Engine. The authentication token is displayed on the last window of the IBM Content Search Services installation program for each server that you install.

To find the authentication token for an installed IBM Content Search Services server:

1. Log on to the host computer as *css_os_user*.
2. From a command prompt, navigate to the *css_install_location/server_name/bin* directory.
3. To find the authentication token, enter `configTool printToken -configPath "css_install_location/server_name/config"`.
4. To generate a new authentication token, enter `configTool generateToken -configPath "css_install_location/server_name/config" -seed token_name`.
5. Store the authentication token and the encryption key in the database if applicable.

Configuring Content Platform Engine for IBM Content Search Services

You must configure IBM Content Search Services as an IBM Content Search Services server on Content Platform Engine.

The IBM Content Search Services server that is configured on Content Platform Engine contains the connection and configuration information for a single IBM Content Search Services server. The IBM Content Search Services server is associated with a site and can be used by any object store in the same site to create and search indexes.

When filtering text from a document, Content Platform Engine places the document in a temporary work directory. This work document is given the same file name extension as the original document. The file system must support the characters that are used in the file name extension. Without this character support, Content Platform Engine generates an error and does not index the document.

For example, if the file name extensions of the Content Platform Engine documents that you want to index contain Japanese characters, you must set the code page of the operating system to support these characters.

“Configuring IBM Content Search Services servers on Content Platform Engine” on page 71

You can configure IBM Content Search Services servers on Content Platform Engine in Index mode, Server mode, or Index And Server mode to search for and index documents, custom objects, folders, and annotations.

“Setting the indexing languages for an object store” on page 71

You need to set the indexing languages on the object store before you can index documents contained in it.

“Creating an index area” on page 72

Index areas contain the IBM Search indexes for the content-based retrieval data that is created, updated, and queried by IBM Content Search Services. You must create index areas in order to search for text within object stores.

“Disabling IBM Legacy Content Search Engine” on page 73

If you created indexes in an object store by using IBM Legacy Content Search Engine in a previous version of FileNet P8, you need to disable (decommission) IBM Legacy Content Search Engine.

“Enabling text search on the object store” on page 73

You can enable text search servers on any object store that resides in the same site as the IBM Content Search Services server.

“Configuring objects that can be indexed for content based retrieval” on page 74

You can configure documents, custom objects, folders, and annotations for content-based retrieval by using IBM Administration Console for Content Platform Engine.

Configuring IBM Content Search Services servers on Content Platform Engine

You can configure IBM Content Search Services servers on Content Platform Engine in Index mode, Server mode, or Index And Server mode to search for and index documents, custom objects, folders, and annotations.

Ensure that the Content Platform Engine server is running before you proceed.

To configure IBM Content Search Services servers on Content Platform Engine:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only IBM Content Search Services configuration values, filter by **ACCE: Content Search Services configuration tab** in the **Installation or Configuration Program** column.

2. Start IBM Administration Console for Content Platform Engine if you did not already do so:
 - a. On any computer, open a browser and navigate to `http://CPE_Server:port/acce`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.
 - b. Log on as the *gcd_admin* user.
3. Configure a text search server for a IBM Content Search Services server:
 - a. In the domain navigation pane, right-click the **Global Configuration > Administration > Text Search Servers** folder and click **New Text Search Server**.
 - b. Complete the wizard.
4. Repeat the preceding steps for the other text search servers.

Setting the indexing languages for an object store

You need to set the indexing languages on the object store before you can index documents contained in it.

Ensure that the Content Platform Engine server is running before you proceed. Also ensure that the IBM Content Search Services servers are configured in the same site as the object store.

To set the indexing languages on an object store:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only IBM Content Search Services configuration values, filter by **ACCE: Content Search Services configuration tab** in the **Installation or Configuration Program** column.

2. Start IBM Administration Console for Content Platform Engine if you did not already do so:

- a. On any computer, open a browser and navigate to `http://CPE_Server:port/acce`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.
 - b. Log on as the *gcd_admin* user.
3. Set the indexing languages.

Restriction: If you do not select indexing languages for the object store, the following error message is displayed when you try to enable text search on the object store: One or more values must be set for the `TextSearchIndexingLanguages` property when IBM Content Search Services is enabled on the object store.

- a. In the navigation pane, open the **Object Stores** folder and select the object store.
- b. In the details pane, click **Text Search**.
- c. In the **Indexing Languages** field, select the desired language codes from the list. Be aware that the languages you select apply only to documents that you subsequently index. If you want the selected languages to apply to already-indexed documents, then you have to reindex the documents.

Creating an index area

Index areas contain the IBM Search indexes for the content-based retrieval data that is created, updated, and queried by IBM Content Search Services. You must create index areas in order to search for text within object stores.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

Ensure that the location of the index area that you create is read- and write-accessible from all IBM Content Search Services servers in these modes: index, search, and dual (index and search).

Restriction: If you do not create an index area for the object store, the error message IBM Content Search Services was not enabled is displayed when you try to enable text search on the object store.

Important: It is a best practice for Content Platform Engine storage areas and IBM Content Search Services full-text indexes to not share the same root directory, disk, or volume. Otherwise, disk I/O contention will cause degraded performance.

To create an index area:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled, and filter by **ACCE: Create an Index Area** in the **Installation or Configuration Program** column.

2. Start IBM Administration Console for Content Platform Engine if you did not already do so:
 - a. On any computer, open a browser and navigate to `http://CPE_Server:port/acce`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.
 - b. Log on as the *gcd_admin* user.

3. Select an object store in the left pane, navigate to **Administrative > Index Areas**, and click **New Index Area** to start the New Index Area wizard.
4. Complete the wizard screens by using the values from your worksheet.
5. Repeat these steps to create additional index areas with different names.

Related tasks:

“Enabling text search on the object store”

You can enable text search servers on any object store that resides in the same site as the IBM Content Search Services server.

Disabling IBM Legacy Content Search Engine

If you created indexes in an object store by using IBM Legacy Content Search Engine in a previous version of FileNet P8, you need to disable (decommission) IBM Legacy Content Search Engine.

To disable IBM Legacy Content Search Engine:

1. Start IBM Administration Console for Content Platform Engine if you did not already do so:
 - a. On any computer, open a browser and navigate to `http://CPE_Server:port/acce`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.
 - b. Log on as the *gcd_admin* user.
2. For each object store in which you want to disable IBM Legacy Content Search Engine, complete the following substeps:
 - a. In the domain navigation pane, select the object store for which you want to disable IBM Legacy Content Search Engine.
 - b. In the details pane, click **Properties**.
 - c. Scroll to the Verity Domain Configuration property, right-click it, and select **Unset Value** to set the property value to null. Setting the value to null causes the index areas, the collections, and the related index requests to be deleted.
3. To determine that all the index requests are deleted, complete the following substeps:
 - a. Browse to `http://CPE_Server:port/FileNet/AutomaticUpgradeStatus`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.
 - b. For each object store, if LCSE Decommission is in the **Upgrade Status** column, then index requests are still being deleted. When LCSE Decommission no longer appears, then no index requests remain for that object store.

Enabling text search on the object store

You can enable text search servers on any object store that resides in the same site as the IBM Content Search Services server.

To enable a text search on an object store:

1. Start IBM Administration Console for Content Platform Engine if you did not already do so:
 - a. On any computer, open a browser and navigate to `http://CPE_Server:port/acce`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.

- b. Log on as the *gcd_admin* user.
2. Enable a text search:
 - a. In the domain navigation pane, select the object store.
 - b. Click the **Text Search** tab and select the **Enable IBM Content Search Services** check box.

Configuring objects that can be indexed for content based retrieval

You can configure documents, custom objects, folders, and annotations for content-based retrieval by using IBM Administration Console for Content Platform Engine.

To enable content-based retrieval (CBR) for all document classes or some subclasses, you can either enable CBR at the document class level or at the level of the individual subclasses.

To configure objects that can be indexed for content-based retrieval:

1. Start IBM Administration Console for Content Platform Engine if you did not already do so:
 - a. On any computer, open a browser and navigate to `http://CPE_Server:port/acce`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.
 - b. Log on as the *gcd_admin* user.
2. In the navigation pane, expand the folder of the object store for which you want to enable content-based retrieval

Important: Nothing is indexed unless you enable CBR on the associated classes. You can index object content for Document and Annotation classes only. You can index property values for all supported CBR-enabled object classes. To designate property values for indexing, you must enable CBR on the property definition and the object class.

3. Select the **Data Design > Classes** folder. You can configure the following object classes for CBR.
 - Document
 - Folder
 - Custom Object
 - Annotation

The Annotation object class is in the **Classes > Other Classes** folder. The other object classes are in the **Classes** folder.

4. For each object class that you want to enable for CBR, complete the following substeps:
 - a. Right-click the object class and choose **Open**.
 - b. If the object class is Custom Object, Document, or Folder, select the **CBR enabled** check box. If the object class is Annotations, scroll to the Is CBR Enabled field, and set its value to True.

Related information:



Indexable object text

You can configure various index object types for content based retrieval.



Setting the CBR-enabled status for a class

You can configure the class of a selected index object for content based retrieval.



Setting the CBR-enabled status for a property

You can configure the properties of a selected index object class for content based retrieval.

Verifying the IBM Content Search Services installation

You can verify that the IBM Content Search Services installation was successful by using IBM Administration Console for Content Platform Engine to create a search index job and checking to see whether the job returns the correct index objects.

In this verification test you send a query that searches for text that you know is in a document. If the query successfully finds the document, then you know that your IBM Content Search Services configuration is working properly. If the query fails, there are some steps at the bottom of the verification test to help you fix the problem.

To verify the IBM Content Search Services installation:

1. Start IBM Administration Console for Content Platform Engine if you did not already do so:
 - a. On any computer, open a browser and navigate to `http://CPE_Server:port/acce`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.
 - b. Log on as the *gcd_admin* user.
2. Make sure that you completed the tasks explained in “Configuring Content Platform Engine for IBM Content Search Services” on page 70
3. Create a document:
 - a. In the navigation pane, under an object store, right-click the **Browse > Root Folder** folder (or one of its subfolders) and choose **New Document**.
 - b. Complete the New Document wizard steps.
4. Submit an index request for the document:
 - a. In the details pane, click the tab for the newly created document.
 - b. Click **Actions**, and choose **Index for Content Search**. Wait a few minutes to allow time for the index request to be submitted and completed.
5. Verify that the document is successfully indexed:
 - a. In the navigation pane, under the object store, click **Search**.
 - b. In the **Search** tab of the details pane, click **SQL Query**.
 - c. Enter the following SQL query in the Query box and click **Search**.

```
SELECT d.This FROM your_class_name d
INNER JOIN ContentSearch c
ON d.This = c.QueriedObject
WHERE CONTAINS(d.*, 'your_search_string')
```
 - d. In the **Search Results** tab, verify that the SQL query found your document.

If your query finds the document you were looking for, then IBM Content Search Services is working properly. If it does not find the document, check the SQL Text

query syntax and issue it again. If it still fails, see [Checking IBM Content Search Services for common errors](#) to carry out initial steps to try to fix the problem.

After you verify the IBM Content Search Services installation, you can create synonyms for your search terms to improve the results of your search queries. By using synonyms, you can search for words that are specific to your organization, such as acronyms and technical jargon.

Related information:



[Setting synonyms](#)

You can create synonyms for your search terms to improve the results of your search queries.



[Checking CSS for common errors](#)

If your IBM Content Search Services verification test fails or you experience other kinds of content search errors, there are some basic things you can check before accessing the troubleshooting system.

Configuring SSL for IBM Content Search Services

IBM Content Search Services can communicate with Content Engine on both secure and nonsecure channels. You can configure IBM Content Search Services to communicate over a secure connection by using the Secure Sockets Layer (SSL) protocol.

Secure Sockets Layer (SSL) is a commonly used protocol that provides secure connections by letting applications that connect over a network authenticate their identity to each other. SSL also encrypts the data that is exchanged between the applications.

With IBM FileNet Content Engine, you can configure secure channels for IBM Content Search Services on different levels. Based on your specific requirements, you can configure SSL on the following levels:

- Encrypt the data that is transmitted over the network
- Perform SSL server authentication
- Verify the host name of the IBM Content Search Services server in Enterprise Manager

Restriction: Each of these levels is dependent on the previous levels. For example, to perform level 3, you must first configure level 1 and level 2.

Note: The person responsible for configuring SSL for IBM Content Search Services must have good SSL configuration experience. For example, they need to know how to use the Java `keytool.exe`, and know how to generate certificates signed by Certificate Authorities.

“Encrypting data transmitted over the network” on page 77

To encrypt the data that is transmitted over the network, you must set up a secure port on the IBM Content Search Services server. Then, you must use Enterprise Manager to specify the secure port number and enable SSL.

“Performing SSL server authentication” on page 78

To perform SSL server authentication, you must deploy certificates on the IBM Content Search Services server and the Content Platform Engine server that are used in the connection. You can deploy either self-signed certificates or certificates that are signed by an external third-party Certificate Authority (CA).

Encrypting data transmitted over the network

To encrypt the data that is transmitted over the network, you must set up a secure port on the IBM Content Search Services server. Then, you must use Enterprise Manager to specify the secure port number and enable SSL.

To encrypt data that is transmitted over the network:

1. Set up a secure port on the IBM Content Search Services server:
 - a. Log on to the host computer as the *css_install_user* user.
 - b. Stop the IBM Content Search Services server if it is running.
 - c. Open a command prompt and navigate to the folder *YourCSSfolder*\bin where *YourCSSfolder* is the folder where you installed the IBM Content Search Services server.
 - d. Enable a secure port by entering the following command (the double quotes are needed when they delimit white space):

```
configTool.bat set -system -configPath "YourCSSfolder\config"
-securePort 8199
```

where 8199 is the secure port number. For example, if *YourCSSfolder* is C:\Program Files\IBM\Content Search Services\CSS Server\, enter the following command:

```
configtool.bat
set -system -configPath "C:\Program Files\IBM\Content Search Services\CSS
Server\config" -securePort 8199
```

Attention:

For AIX, HP-UX, Linux, Linux for System z, or Solaris users, if *YourCSSfolder* is /opt/IBM/Content Search Services/CSS Server/, enter the following command:

```
configTool.sh
set -system -configPath "/opt/IBM/ContentSearchServices/CSS_Server/config"
-securePort 8199
```

- e. Optional: Disable the nonsecure port after completing all SSL configuration changes. To set the nonsecure port number to 0, enter `configtool.bat set -system -configPath "YourCSSfolder\config" -adminHTTPPort 0`. For AIX, Linux, Linux for System z, or Solaris users, enter `configTool.sh set -system -configPath "YourCSSfolder/config" -adminHTTPPort 0`.
 - f. Start the IBM Content Search Services server.
2. Start IBM Administration Console for Content Platform Engine if you did not already do so:
 - a. On any computer, open a browser and navigate to `http://CPE_Server:port/acce`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.
 - b. Log on as the *gcd_admin* user.
3. Specify the secure port number and enable SSL on the IBM Content Search Services server:
 - a. In the navigation pane of IBM Administration Console for Content Platform Engine select the domain, and navigate to **Global Configuration > Administration > Text Search Servers**.
 - b. In the details pane, select the text search server and click **General**.
 - c. In the Port field, enter the secure port number.
 - d. Click **Properties**.

- e. Set the Is SSL Enabled field value to True.
- f. Set the Validate Server Certificate and the Validate Certificate Host field values to False.

Performing SSL server authentication

To perform SSL server authentication, you must deploy certificates on the IBM Content Search Services server and the Content Platform Engine server that are used in the connection. You can deploy either self-signed certificates or certificates that are signed by an external third-party Certificate Authority (CA).

“Deploying server certificates on IBM Content Search Services server”

You must secure the IBM Content Search Services server end of the connection. Deploy server certificates to the keystore on the IBM Content Search Services server and configure the IBM Content Search Services server to use this keystore.

“Deploying CA certificates on Content Platform Engine server” on page 80

You must secure the Content Platform Engine server end of the connection. Deploy CA certificates to the key store on the Content Platform Engine server and configure the Content Platform Engine server to use this keystore.

“Validating certificates” on page 81

After you deploy the certificates on IBM Content Search Services and Content Platform Engine, you must validate these certificates for IBM Content Search Services by using IBM Administration Console for Content Platform Engine.

“Configuring the Content Platform Engine server to do host validation” on page 82

After you configure the Content Platform Engine server to encrypt data and do SSL server authentication, you can configure the Content Platform Engine server to do host validation for the IBM Content Search Services server.

Deploying server certificates on IBM Content Search Services server:

You must secure the IBM Content Search Services server end of the connection. Deploy server certificates to the keystore on the IBM Content Search Services server and configure the IBM Content Search Services server to use this keystore.

Select the type of server certificate to deploy on the IBM Content Search Services server.

1. Deploying a self-signed server certificate:
 - a. Stop the IBM Content Search Services server if it is running.
 - b. Set the path to your *JRE* bin directory by entering the following command:
set PATH=C:\YourJRE\bin;%PATH% where the bin location is C:\YourJRE\bin.
 - c. Open a command prompt and navigate to the folder *YourCSSFolder*\bin where *YourCSSFolder* is the folder where you installed the IBM Content Search Services server.
 - d. Generate a self-signed server certificate by entering the following command:
keytool -genkey -alias cssSelfsigned -keypass *YourKeyPassword* -keystore selfsignedServerStore -storepass *YourStorePassword* -validity *NumberOfDays* -dname "CN=*YourHostName*, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown".

Restriction: If you plan to verify the host name later, you must include the following parameter:

```
-dname
"CN=YourHostName,OU=Unknown,O=Unknown,L=Unknown,ST=Unknown,C=Unknown"
```

For example, if you want to set the keystore password and the certificate password to changeit, the certificate valid time to 3650 days (10 years), and the host name to Host1, enter the following command:

```
keytool -genkey
        -alias cssSelfsigned -keypass changeit -keystore selfsignedServerStore
        -storepass changeit -validity 3650 -dname "CN=Host1, OU=Unknown, O=Unknown,
        L=Unknown, ST=Unknown, C=Unknown"
```

- e. Verify that the certificate was created in the keystore by entering the following command: `keytool -list -v -keystore selfsignedServerStore -storepass YourStorePassword`.
 - f. Deploy the keystore to IBM Content Search Services by entering the following command: `configTool.bat set -system -configPath YourCSSfolder\config -keyStoreName selfsignedServerStore -keyStorePassword YourStorePassword`. For example, if *YourCSSfolder* is C:\Program Files\IBM\Content Search Services\CSS Server and your keystore password is changeit, enter the following command:


```
keytool -genkey
        -alias cssSelfsigned -keypass changeit -keystore selfsignedServerStore
        -storepass changeit -validity 3650 -dname "CN=Host1, OU=Unknown,
        O=Unknown, L=Unknown, ST=Unknown, C=Unknown"

configTool.bat
set -system -configPath "C:\Program Files\IBM\Content Search Services\CSS
Server\config" -keyStoreName selfsignedServerStore -keyStorePassword
changeit
```
 - g. Start the IBM Content Search Services server.
2. Deploying a third-party server certificate:
- a. Stop the IBM Content Search Services server if it is running.
 - b. Set the path to your *JRE* bin directory by entering the following command: `set PATH=C:\YourJRE\bin;%PATH%` where the bin location is C:\YourJRE\bin.
 - c. Open a command prompt and navigate to the folder *YourCSSfolder\bin* where *YourCSSfolder* is the folder where you installed the IBM Content Search Services server.
 - d. Generate a third-party server certificate by entering the following command:


```
keytool -genkey -alias cssThirdParty -keypass YourKeyPassword
        -keystore thirdPartyServerStore -storepass YourStorePassword
        -validity NumberOfDays -dname "CN=YourHostName, OU=Unknown,
        O=Unknown, L=Unknown, ST=Unknown, C=Unknown"
```

Restriction: If you plan to verify the host name later, you must include the following parameter:

```
-dname "CN=YourHostName,OU=Unknown, O=Unknown,
L=Unknown, ST=Unknown, C=Unknown"
```

For example, if you want to set the keystore password and the certificate password to changeit, the certificate valid time to 3650 days (10 years), and the host name to Host1, enter the following command:

```
keytool
        -genkey -alias cssThirdParty -keypass changeit
        -keystore thirdPartyServerStore -storepass changeit
        -validity 3650 -dname "CN=Host1, OU=Unknown, O=Unknown,
        L=Unknown, ST=Unknown, C=Unknown"
```

- e. Verify that the certificate was created in the keystore by entering the following command: `keytool -list -v -keystore thirdPartyServerStore -storepass YourStorePassword`.

- f. Generate a certificate request, by entering the following command: `keytool -certreq -alias cssThirdParty -keypass YourKeyPassword -keystore thirdPartyServerStore -storepass YourStorePassword -dname "CN=YourHostName, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown" -file certRequest.txt`
- g. Go to a Certificate Authority (CA) website and use this request to get a server certificate.
- h. Save the server certificate on the IBM Content Search Services server in the *YourCSSfolder*\bin directory. For example, save the certificate file as *certnew.p7b*.
- i. Open a command prompt and navigate to the *YourCSSfolder*\bin folder.
- j. Import the certificate to keystore *thirdPartyServerStore*, by entering the following command: `keytool -import -alias cssThirdParty -keystore thirdPartyServerStore -storepass YourStorePassword -file certnew.p7b`.
- k. Verify that the certificate was imported in the keystore by entering the following command: `keytool -list -v -keystore thirdPartyServerStore -storepass YourStorePassword`.
- l. Deploy the keystore to the IBM Content Search Services server by entering the following command: `configTool.bat set -system -configPath YourCSSfolder\config -keyStoreName thirdPartyServerStore -keyStorePassword YourStorePassword`. For example, if *YourCSSfolder* is C:\Program Files\IBM\Content Search Services\CSS Server and your keystore password is *changeit*, you enter the following command:

```
configTool.bat
set -system -configPath "C:\Program Files\IBM\Content Search Services\CSS
Server\config" -keyStoreName thirdPartyServerStore -keyStorePassword
changeit
```
- m. Start the IBM Content Search Services server.

Deploying CA certificates on Content Platform Engine server:

You must secure the Content Platform Engine server end of the connection. Deploy CA certificates to the key store on the Content Platform Engine server and configure the Content Platform Engine server to use this keystore.

Select the type of CA certificate to deploy on the Content Platform Engine server.

1. Deploying a self-signed CA certificate:
 - a. On the IBM Content Search Services server, open a command prompt and navigate to *YourCSSfolder*\bin folder, where *YourCSSfolder* is the folder where you installed the IBM Content Search Services server.
 - b. Export the certificate to a file by entering the following command: `keytool -export -alias cssSelfsigned -keypass YourKeyPassword -keystore selfsignedServerStore -storepass YourStorePassword -file selfsignedCert.cer`.
 - c. Copy the *selfsignedCert.cer* file to a folder on the Content Platform Engine server, for example, C:\IBM\cssKeystore.
 - d. On the Content Platform Engine server, open a command prompt and navigate to the C:\IBM\cssKeystore folder.

- e. Deploy the selfsignedCert.cer file to keystore selfsignedCaStore by entering the following command: `keytool -import -alias cssSelfsigned -keystore selfsignedCaStore -storepass YourStorePassword -file selfsignedCert.cer`.
 - f. Verify that the certificate was created in the keystore by entering the following command: `keytool -list -v -keystore selfsignedCaStore -storepass YourStorePassword`.
 - g. To perform SSL authentication, specify the following Java system parameters on the Content Platform Engine application server. For more information about adding Java system parameters, see your application server documentation.
 - `-Djavax.net.ssl.trustStore=C:\IBM\cssKeyStore\selfsignedCaStore`
 - `-Djavax.net.ssl.trustStorePassword=YourStorePassword`
 - If your application server is WebSphere, edit the file `WAS_HOME/java/jre/lib/security/java.security` and set `keystore.type=pkcs12`. If your application server is clustered, perform this step on each Content Platform Engine node.
 - h. Restart the Content Platform Engine application server instance.
2. Deploying a third-party CA certificate:
- a. Download a CA certificate from the Certificate Authority web site and save it as `ca.cer` in any folder on your Content Platform Engine server, for example, `C:\IBM\cssKeyStore`.
 - b. On the Content Platform Engine server, open a command prompt and navigate to the `C:\IBM\cssKeyStore` folder.
 - c. Deploy the `ca.cer` file to keystore `thirdPartyCaStore` by entering the following command, `keytool -import -alias cssThirdParty -keystore thirdPartyCaStore -storepass YourStorePassword -file ca.cer`.
 - d. Verify that the certificate was imported into the keystore by entering the following command, `keytool -list -v -keystore thirdPartyCaStore -storepass YourStorePassword`.
 - e. To perform SSL authentication, specify the following Java system parameters on the Content Platform Engine application server. For more information about adding Java system parameters, see your application server documentation.
 - `-Djavax.net.ssl.trustStore=C:\IBM\cssKeyStore\thirdPartyCaStore`
 - `-Djavax.net.ssl.trustStorePassword=YourStorePassword`
 - If your application server is WebSphere, edit the file `WAS_HOME/java/jre/lib/security/java.security` and set `keystore.type=pkcs12`. If your application server is clustered, perform this step on each CE node.
 - f. Restart the Content Platform Engine application server instance.

Related tasks:

Starting or stopping an application server instance

Validating certificates:

After you deploy the certificates on IBM Content Search Services and Content Platform Engine, you must validate these certificates for IBM Content Search Services by using IBM Administration Console for Content Platform Engine.

To validate certificates for IBM Content Search Services:

1. Start IBM Administration Console for Content Platform Engine if you did not already do so:
 - a. On any computer, open a browser and navigate to `http://CPE_Server:port/acce`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.
 - b. Log on as the *gcd_admin* user.
2. Validate the certificates for IBM Content Search Services:
 - a. In the navigation pane, expand the domain node.
 - b. Navigate to **Global Configuration > Administration > Text Search Servers**.
 - c. Select a text search server.
 - d. In the details pane, click **General** and scroll to the Communication Security field.
 - e. Select the following check boxes:
 - Enable use of the Secure Sockets Layer (SSL) protocol
 - Validate the SSL server certificate
 - Validate the SSL certificate host
3. Repeat the preceding steps for the other text search servers.

Configuring the Content Platform Engine server to do host validation:

After you configure the Content Platform Engine server to encrypt data and do SSL server authentication, you can configure the Content Platform Engine server to do host validation for the IBM Content Search Services server.

To configure the Content Platform Engine server to do host validation:

1. Start IBM Administration Console for Content Platform Engine if you did not already do so:
 - a. On any computer, open a browser and navigate to `http://CPE_Server:port/acce`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.
 - b. Log on as the *gcd_admin* user.
2. In the navigation pane of Administration Console for Content Platform Engine, expand your FileNet P8 domain. Within the domain, expand the folders **Global Configuration > Administration > Text Search Servers** and click the icon of one of the text search servers.
3. In the details pane, click the name of the text search server, scroll to the **Communication Security** section, and select the following check boxes:
 - Enable use of the Secure Sockets Layer (SSL) protocol
 - Validate the SSL server certificate
 - Validate the SSL certificate host
4. Repeat these steps for the other text search servers in your domain.

Installing and configuring Application Engine

Application Engine provides a client application called Workplace that you can use to access the information managed by Content Platform Engine. After you install the server, you must also configure your application server to work with Application Engine, and deploy the application.

As an alternative to the Application Engine component and its Workplace user application, you can set up Workplace XT or IBM Content Navigator. See for more details on IBM Content Navigator.

If you are installing FileNet P8 for IBM Case Manager, you must install Workplace XT. See the Workplace XT documentation for details.

1. "Installing Application Engine" on page 84
To enable the web client application, Workplace, install Application Engine on a supported web application server. To complete the installation, provide the necessary parameter values to enable Workplace to access the information that is managed by Content Platform Engine.
2. "Installing Application Engine software updates" on page 88
If any required fix packs and interim fixes exist for Application Engine, you must install these software updates.
3. "Installing the latest Content Platform Engine Client files on Application Engine servers" on page 89
The Content Platform Engine Client software enables communication between the Application Engine and Content Platform Engine. Install the latest release or fix pack version of the Content Platform Engine Client files on all Application Engine servers.
4. "Configuring Application Engine on the application server" on page 91
After you complete the Application Engine installation, you must configure Application Engine files and your application sever to enable communication between Application Engine and Content Platform Engine. You can choose the appropriate configuration tasks for your application server type and environment.
5. "Deploying Application Engine on the application server" on page 103
After you install and configure Application Engine, you must deploy your client application, Workplace, on your application server. You might be required to re-create the WAR or WAR and EAR files before you deploy.
6. "Setting Application Engine bootstrap preferences" on page 107
By successfully signing in to Workplace and saving the bootstrap preferences, you verify basic Application Engine functionality such as user authentication as well as communication and storing of data in Content Engine.
7. "Updating Application Engine settings in a load balanced environment" on page 111
You can update Application Engine settings in a load balanced Application Engine environment consisting of a load balancer or proxy device, several HTTP servers and several application server instances.

Installing Application Engine

To enable the web client application, Workplace, install Application Engine on a supported web application server. To complete the installation, provide the necessary parameter values to enable Workplace to access the information that is managed by Content Platform Engine.

Assume any references to the Content Engine in these topics apply to the Content Platform Engine.

Important: In a high availability environment, you must install Application Engine on all nodes in the application server configuration. Even in an application server cluster configuration the Application Engine provides components that run outside of the application server. These are only available through an Application Engine installation.

If you plan to install and use the IBM FileNet Workplace XT product, you do not need to install Application Engine.

To ensure proper functionality and performance, only install one instance of Application Engine per application server (or virtual machine or WebSphere Application Server LPAR). You can, however, deploy multiple instances of a single Application Engine version per application server.

Before logging on to Workplace for the first time, at least one object store must exist on the Content Platform Engine to hold the site preferences. See “Creating the initial object store” on page 59 for more information.

Red Hat Enterprise Linux 5.x has a security feature that can cause errors during installation. For details on resolving the issue before you install, see the *IBM FileNet P8 Hardware and Software Requirements*. In the guide, search for “SELinux”.

Important: Do NOT install this component unless it is supported at the release levels of your FileNet P8 environment. For information, see the *IBM FileNet P8 Hardware and Software Requirements* and the *IBM FileNet P8 Compatibility Matrix* documents.

“Installing Application Engine interactively” on page 85

You can use the installation wizard to install Application Engine. To complete the installation, provide the necessary parameter values to enable the Application Engine client application, Workplace, to access the information that is managed by Content Engine.

“Installing Application Engine silently” on page 86

You can include the parameters for your Application Engine installation in a silent input file, and then run the installation from a command line.

“Verifying your Application Engine installation” on page 88

You can verify your Application Engine installation by using Workplace.

Related information:



Configuring JBoss Application Server clusters

JBoss Application Server servers can be grouped together into a cluster for performance or to provide high availability.

Installing Application Engine interactively

You can use the installation wizard to install Application Engine. To complete the installation, provide the necessary parameter values to enable the Application Engine client application, Workplace, to access the information that is managed by Content Engine.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

Important: In a high availability environment, you must install Application Engine on all nodes in the application server configuration. Even in an application server cluster configuration the Application Engine provides components that run outside of the application server such as the Component Manager. These are only available through an Application Engine installation.

To install the Application Engine software interactively:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Content Engine values, filter by **AE Installer** in the **Installation or Configuration Program** column.

2. In a highly available environment, mount the shared configuration directory from all nodes in the application server configuration.

When the location of the shared configuration directory is decided, that directory must be mounted and accessible from all servers in the application server configuration. Also, ensure that the same directory path is used on all systems. If the path on the first system is:

`//home/AE/Config`

make sure this same path is available on all other systems.

3. (Highly available environments using IBM WebSphere Application Server or Oracle WebLogic Server) Verify that your application farm or cluster configuration is running.
4. Log on to the application server, as appropriate for your operating system:

Option	Description
AIX, HPUX, Linux, Linux on System z, Solaris	Log on as a user with read, write, and execute access to the directory where you plan to install Application Engine.

5. Access the IBM FileNet P8 Application Engine 4.0.2.0 installation software.
6. Start the installation program.

Table 21. Starting the installation program

Platform	Command
Linux	P8AE-4.0.2.0-LINUX.bin

7. Complete the Application Engine installer screens by using the values from your worksheet.

Note: In high availability environments, specify the location to hold the Application Engine shared configuration data on the Specify Configuration Directory screen. On the Content Engine API Configuration screen, make sure to specify the proper Content Engine URLs following the format and examples shown in “Content Platform Engine in an application server cluster by using EJB transport” on page 61.

8. View the `app_engine_install_log_4_0_2.txt` file, located in `AE_install_path/AE/Logs`.

Verify that no errors or failures were logged. Look for the ERROR designation at the start of a line. Correct any errors before you proceed.

9. In highly available environments, you need to synchronize the `UTCryptoKeyFile.properties` file across your Application Engine nodes.

Each participating Application Engine server must use the same encryption key file. Copy the `UTCryptoKeyFile.properties` file installed on the first Application Engine server in your farm to all the other servers in your farm.

For information, see the FileNet P8 Developer Help topic **Developing IBM FileNet applications > Workplace Development > Workplace Customization Guide > User Tokens > Configuring Applications to Use Tokens**.

Related concepts:



Installation and upgrade worksheet

For more information about the installation and upgrade worksheet, see the worksheet topics in *Plan and Prepare Your Environment for IBM FileNet P8*.

Related information:



Creating a local or shared directory for the shared configuration files

You can create a local or shared directory for the shared configuration files in highly available environments.

Installing Application Engine silently

You can include the parameters for your Application Engine installation in a silent input file, and then run the installation from a command line.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

Important: In a high availability environment, you must install Application Engine on all nodes in the application server configuration. Even in an application server cluster configuration the Application Engine provides components that run outside of the application server such as the Component Manager. These are only available through an Application Engine installation.

To install the Application Engine software silently:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Content Engine values, filter by **AE Installer** in the **Installation or Configuration Program** column.

2. In a highly available environment, mount the shared configuration directory from all nodes in the application server configuration.

When the location of the shared configuration directory is decided, that directory must be mounted and accessible from all servers in the application

server configuration. Also, ensure that the same directory path is used on all systems. If the path on the first system is:

`//home/AE/Config`

make sure this same path is available on all other systems.

3. (Highly available environments using IBM WebSphere Application Server or Oracle WebLogic Server) Verify that your application farm or cluster configuration is running.
4. Log on to the application server, as appropriate for your operating system:

Option	Description
AIX, HPUX, Linux, Linux on System z, Solaris	Log on as a user with read, write, and execute access to the directory where you plan to install Application Engine.

5. Locate the IBM FileNet P8 Application Engine 4.0.2 installation software package, and copy the appropriate `AE_silent_input.txt` file to a local directory.
6. Follow the instructions in the silent input file to edit the file to reflect the appropriate responses for your installation. Use the values in your worksheet.

Important: If you are modifying the silent input file to perform an upgrade from Application Engine 3.5 to Application Engine 4.0.2 you must modify all instances of `AE_install_path` in the script as follows:

AIX, HPUX, Linux, Linux on System z, Solaris

Change `../FileNet/AE` to `../FileNet`

Note: In high availability environments, specify the location to hold the Application Engine shared configuration data. For Content Engine configuration, make sure to specify the proper Content Engine URLs following the format and examples shown in “Content Platform Engine in an application server cluster by using EJB transport” on page 61.

7. From a command prompt, navigate to and run the installer.

AIX, HPUX, Linux, Linux on System z, Solaris

`./P8AE-4.0.2.0-operating system.bin -options
path_to_edited_input_file/AE_silent_input.txt -silent`

8. View the `app_engine_install_log_4_0_2.txt` file, located in `AE_install_path/AE/Logs`.


Verify that no errors or failures were logged. Look for the ERROR designation at the start of a line. Correct any errors before you proceed.

9. In highly available environments, you need to synchronize the `UTCryptoKeyFile.properties` file across your Application Engine nodes.

Each participating Application Engine server must use the same encryption key file. Copy the `UTCryptoKeyFile.properties` file installed on the first Application Engine server in your farm to all the other servers in your farm.

For information, see the FileNet P8 Developer Help topic **Developing IBM FileNet applications > Workplace Development > Workplace Customization Guide > User Tokens > Configuring Applications to Use Tokens**.

Related concepts:

 Installation and upgrade worksheet

For more information about the installation and upgrade worksheet, see the worksheet topics in *Plan and Prepare Your Environment for IBM FileNet P8*.

Related information:

 Creating a local or shared directory for the shared configuration files

You can create a local or shared directory for the shared configuration files in highly available environments.

Verifying your Application Engine installation

You can verify your Application Engine installation by using Workplace.

To verify Application Engine installation:

1. Sign in to Workplace:
 - a. On any computer, open a browser and type:
`http://ApplicationEngineServerName:port#/Workplace`
- Important:** *ApplicationEngineServerName* cannot be localhost or an IP address.
- b. Enter a user name and password, and then click **Sign in**.
 2. Use Workplace to browse, search, add a document, and view the Tasks page.
 3. In a high availability environment, by using the application server administration tool, verify that the Application Engine application is running.
 - a. Open a Web browser and type in the URL for the Application Engine application.
 - If you are using a load-balancer or proxy server the URL has the form:

Application Engine

`http://virtual_name:port_number/Workplace`

- If connecting to an individual cluster node the URL would have the form:

Application Engine

`http://clustered_server_name:port_number/Workplace/`

Sign-in by using the virtual name to properly set the base Application Engine URL. If it is not set correctly you must change it in Site Preferences.

- b. Verify that the sign-in page displays, and log in as a user.
 - c. Fail one of the nodes.
 - d. Verify that you can reload the sign-in page, and log in as the same user.
4. To verify Application Engine is running on a single server installation:
 - a. Access the following URL:
`http://cpit_server:9080/Workplace`
 - b. Log in with the credentials provided in *install_path/IBM/cpit/readme.txt*.
 - c. Use Workplace to browse, search, add a document, and view the Tasks page.

Installing Application Engine software updates

If any required fix packs and interim fixes exist for Application Engine, you must install these software updates.

Remember: In farm and cluster environments, install Application Engine software updates on all nodes.

To install the Application Engine software updates:

1. Access the IBM FileNet P8 Platform support site to obtain the latest Application Engine software updates.
2. Open the readmes for any subsequent fix packs or interim fixes (typically optional) and perform the installation procedures provided.

Installing the latest Content Platform Engine Client files on Application Engine servers

The Content Platform Engine Client software enables communication between the Application Engine and Content Platform Engine. Install the latest release or fix pack version of the Content Platform Engine Client files on all Application Engine servers.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.


“Installing the latest Content Platform Engine Client files on Application Engine servers interactively”

The installation wizard provides an interactive way to install the Content Platform Engine Client files. You can use the values from your worksheet to fill in the required value for each field on the wizard screens.

“Installing the latest Content Platform Engine Client files on Application Engine servers silently” on page 90

The command-line method provides a way to silently install the Content Platform Engine Client files. You can use the values in your installation worksheet to edit the silent input text file before you run the installation.

Related concepts:

 Installation and upgrade worksheet

For more information about the installation and upgrade worksheet, see the worksheet topics in *Plan and Prepare Your Environment for IBM FileNet P8*.

Installing the latest Content Platform Engine Client files on Application Engine servers interactively

The installation wizard provides an interactive way to install the Content Platform Engine Client files. You can use the values from your worksheet to fill in the required value for each field on the wizard screens.

Important: Be sure that Content Platform Engine is running before you start installing Content Platform Engine Client files.

To install the Content Platform Engine Client files interactively:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Content Platform Engine values, filter by **CE Client Installer** in the **Installation or Configuration Program** column.

2. On the machine where Application Engine is installed, log on as any user who has the following permissions:

- Read and write permission to a temporary directory, such as temp (Windows) or tmp (AIX, HPUX, HPUNIX, Linux, Linux for System z, or Solaris), on the machine where Application Engine is installed
 - Execute permission on the Content Platform Engine client install software
3. Copy the Content Platform Engine client installation software from the Content Platform Engine installation software to the temporary directory. The version of the client installation software must match the version of Content Platform Engine.
 4. Expand the compressed Content Platform Engine client installation software file in the temporary directory.
 5. Access the Content Platform Engine client update software in the temporary directory.
 6. Run the following command:

Table 22. Content Platform Engine installation command


Operating System	Install Program
Linux	5.2.0-P8CE-CLIENT-LINUX.BIN

7. Complete the installation screens by using the values from your worksheet.
8. Complete the installation program wizard by using the values from your worksheet.
9. When the installation completes, check the Content Platform Engine Client log file for errors. The path to the log file depends on the type of operating system on the machine where you installed the Content Platform Engine client files:

Table 23. Log file path

Operating System	Path to Log File
AIX, HPUX, HPUNIX, Linux, Linux for System z, Solaris	/opt/IBM/FileNet/CEClient/ ceclient_install_log_5.2.0.txt

Related concepts:

 Installation and upgrade worksheet

For more information about the installation and upgrade worksheet, see the worksheet topics in *Plan and Prepare Your Environment for IBM FileNet P8*.

Installing the latest Content Platform Engine Client files on Application Engine servers silently

The command-line method provides a way to silently install the Content Platform Engine Client files. You can use the values in your installation worksheet to edit the silent input text file before you run the installation.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

Important: Be sure that Content Platform Engine is running before you start installing Content Platform Engine Client files.

To install the latest Content Platform Engine Client files on Application Engine servers silently:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Content Platform Engine values, filter by **CE Client Installer** in the **Installation or Configuration Program** column.

2. On the machine where Application Engine is installed, log on as any user who has the following permissions:
 - Read and write permission to a temporary directory, such as temp (Windows) or tmp (AIX, HPUX, HPUXi, Linux, Linux for System z, or Solaris), on the machine where Application Engine is installed
 - Execute permission on the Content Platform Engine client install software
3. Copy the Content Platform Engine client installation software from the Content Platform Engine installation software to the temporary directory. The version of the client installation software must match the version of Content Platform Engine.
4. Expand the compressed Content Platform Engine client installation software file in the temporary directory.
5. Make a backup copy of the ceclient_silent_install.txt input file in the temporary directory.
6. Open the silent input file in a text editor. Follow the instructions in the silent input file to edit the file to reflect the appropriate responses for your update. Use the values from your worksheet.
7. Navigate to the temporary directory path containing the Content Platform Engine client installation program, and run the following command, where:
path is the path that contains the installation program.

Table 24. Content Platform Engine client installation program


Operating System	Install Program
Linux	5.2.0-P8CE-CLIENT-LINUX.BIN -f <i>path</i> /CEClient.Linux/ ceclient_silent_install.txt -i silent

8. When the installation completes, check the Content Platform Engine Client log file for errors. The path to the log file depends on the type of operating system on the machine where you installed the Content Platform Engine client files:

Table 25. Log file path

Operating System	Path to Log File
AIX, HPUX, HPUXi, Linux, Linux for System z, Solaris	/opt/IBM/FileNet/CEClient/ ceclient_install_log_5.2.0.txt

Related concepts:

 Installation and upgrade worksheet

For more information about the installation and upgrade worksheet, see the worksheet topics in *Plan and Prepare Your Environment for IBM FileNet P8*.

Configuring Application Engine on the application server

After you complete the Application Engine installation, you must configure Application Engine files and your application sever to enable communication between Application Engine and Content Platform Engine. You can choose the appropriate configuration tasks for your application server type and environment.

(Farm of independent application server instances) Configure and deploy the Application Engine on each node. When installing in farm of independent

application server instances, the steps shown for deploying Application Engine on the application server must be performed on every node.

Important: Since there is no central administration server, every server acts as a separate server instance and must be configured as such.

“Configuring Application Engine on WebSphere Application Server”

After you install the Application Engine server, you must configure WebSphere Application Server to work with Application Engine. You can also configure changes for optional modes like SSO.

Configuring Application Engine on WebSphere Application Server

After you install the Application Engine server, you must configure WebSphere Application Server to work with Application Engine. You can also configure changes for optional modes like SSO.

Remember: In farm and cluster environments, configure Application Engine on WebSphere Application Server on all nodes.

“Editing web.xml for container-managed authentication” on page 93

You can choose to use WebSphere Application Server with container-managed authentication. To enable this optional authentication approach, edit the web.xml file on the WebSphere Application Server.

“Editing web.xml for SSO” on page 95

You can use SSO with a proxy server in your Application Engine environment. To enable this optional approach, edit the web.xml file on the WebSphere Application Server.

“Configuring Java Virtual Machine settings for JAAS login and memory” on page 98

Use the Java Virtual Machine settings in the WebSphere Application Server to set up JAAS login information for authentication and memory settings for resource usage.

“Configuring Lightweight Third Party Authentication (LTPA)” on page 99

To set up LTPA security, configure settings to match on both the Content Platform Engine application server and the Application Engine application server. If your Application Engine and Content Platform Engine are on the same WebSphere Application Server, you are not required to configure LTPA.

“Configuring stand-alone Lightweight Directory Access Protocol (LDAP)” on page 101

To enable LDAP communication between Application Engine and Content Engine, you must configure settings on the WebSphere Application Server. It is recommended that the LDAP configuration settings match those set on the application server where Content Engine is installed.

“Configuring Lightweight Directory Access Protocol (LDAP) for federated repositories” on page 102

If you have a multiple domain environment, configure LDAP settings for federated repositories on the WebSphere Application Server to enable LDAP communication between Application Engine and Content Engine. It is recommended that the LDAP configuration settings match those set on the application server where Content Engine is installed.

Editing web.xml for container-managed authentication

You can choose to use WebSphere Application Server with container-managed authentication. To enable this optional authentication approach, edit the web.xml file on the WebSphere Application Server.

1. Make a backup copy of web.xml.

AE_install_path/Workplace/WEB-INF/web.xml

2. Open web.xml for editing, search for the parameter challengeProxyEnabled, and set it to false.

```
<param-name>challengeProxyEnabled</param-name>
<param-value> false </param-value>
```

3. Search for the first instance of <web-resource-collection>, and uncomment the <url-pattern> as noted in the file comments.

```
<web-resource-collection>
<web-resource-name>action</web-resource-name>
<description>Define the container secured resource</description>
<url-pattern>/containerSecured/*</url-pattern>
```

```
<!--
```

Uncomment this section if all resources that require credentials must be secured in order to obtain a secured Thread. If using WebSphere, this section must be uncommented. --> Move this commenting tag here from just before the </web-resource-collection> closing tag below.

```
<url-pattern>/containerSecured/*</url-pattern>
<url-pattern>/</url-pattern>
<url-pattern>/author/*</url-pattern>
<url-pattern>/Browse.jsp</url-pattern>
<url-pattern>/eprocess/*</url-pattern>
<url-pattern>/Favorites.jsp</url-pattern>
<url-pattern>/GetPortalSitePreferences.jsp</url-pattern>
<url-pattern>/GetTokenSignIn.jsp</url-pattern>
<url-pattern>/GetUserInformation.jsp</url-pattern>
<url-pattern>/GetUserToken.jsp</url-pattern>
<url-pattern>/HomePage.jsp</url-pattern>
<url-pattern>/IntegrationWebBasedHelp.jsp</url-pattern>
<url-pattern>/is/*</url-pattern>
<url-pattern>/operations/*</url-pattern>
<url-pattern>/properties/*</url-pattern>
<url-pattern>/redirect/*</url-pattern>
<url-pattern>/regions/*</url-pattern>
<url-pattern>/Search.jsp</url-pattern>
<url-pattern>/select/*</url-pattern>
<url-pattern>/SelectReturn.jsp</url-pattern>
<url-pattern>/Tasks.jsp</url-pattern>
<url-pattern>/UI-INF/*</url-pattern>
<url-pattern>/utils/*</url-pattern>
<url-pattern>/WcmAdmin.jsp</url-pattern>
<url-pattern>/WcmAuthor.jsp</url-pattern>
<url-pattern>/WcmBootstrap.jsp</url-pattern>
<url-pattern>/WcmCloseWindow.jsp</url-pattern>
<url-pattern>/WcmDefault.jsp</url-pattern>
<url-pattern>/WcmError.jsp</url-pattern>
<url-pattern>/WcmJavaViewer.jsp</url-pattern>
<url-pattern>/WcmObjectBookmark.jsp</url-pattern>
<url-pattern>/WcmQueueBookmark.jsp</url-pattern>
<url-pattern>/WcmSignIn.jsp</url-pattern>
<url-pattern>/WcmSitePreferences.jsp</url-pattern>
<url-pattern>/WcmUserPreferences.jsp</url-pattern>
<url-pattern>/WcmWorkflowsBookmark.jsp</url-pattern>
<url-pattern>/wizards/*</url-pattern>
<url-pattern>/Author/*</url-pattern>
<url-pattern>/axis/*.jws</url-pattern>
<url-pattern>/Browse/*</url-pattern>
```

```

<url-pattern>/ceTunnel</url-pattern>
<url-pattern>/CheckoutList/*</url-pattern>
<url-pattern>/downloadMultiTransferElement/*</url-pattern>
<url-pattern>/ExternalUrl/*</url-pattern>
<url-pattern>/findRecordTarget</url-pattern>
<url-pattern>/formCallback/*</url-pattern>
<url-pattern>/getAnnotSecurity/*</url-pattern>
<url-pattern>/getCEAnnotations/*</url-pattern>
<url-pattern>/getContent/*</url-pattern>
<url-pattern>/getForm/*</url-pattern>
<url-pattern>/getISAnnotations/*</url-pattern>
<url-pattern>/getISAnnotSecurity/*</url-pattern>
<url-pattern>/getISContent/*</url-pattern>
<url-pattern>/getMultiContent/*</url-pattern>
<url-pattern>/getPreview</url-pattern>
<url-pattern>/getProcessor/*</url-pattern>
<url-pattern>/getRealms/*</url-pattern>
<url-pattern>/getUsersGroups/*</url-pattern>
<url-pattern>/Inbox/*</url-pattern>
<url-pattern>/integrationCommandProxy</url-pattern>
<url-pattern>/integrationResponse</url-pattern>
<url-pattern>/integrationResponseProxy</url-pattern>
<url-pattern>/integrationWebBasedCommand</url-pattern>
<url-pattern>/keepAlive</url-pattern>
<url-pattern>/launch/*</url-pattern>
<url-pattern>/PublicQueue/*</url-pattern>
<url-pattern>/putContent/*</url-pattern>
<url-pattern>/QuickSearch/*</url-pattern>
<url-pattern>/signingServlet/*</url-pattern>
<url-pattern>/transport/*</url-pattern>
<url-pattern>/upload/*</url-pattern>
<url-pattern>/vwsimsoapervlet</url-pattern>
<url-pattern>/vwsoaprouter</url-pattern>
<url-pattern>/Workflows/*</url-pattern>
Move the closing comment tag from
here to the location indicated at the beginning of this example.
</web-resource-collection>

```

4. Locate the section <auth-constraint>, comment the wildcard (*) <role-name> as noted in the file comments.

```

<auth-constraint>
<!-- <role-name>*</role-name> -->
<!-- For WebSphere 6, use
the role-name line below instead of the wildcard role above.
-->

<role-name>All Authenticated</role-name>

<!-- For WebSphere 6, add this
security-role element below the login-config element (below).
<security-role>
<description>All Authenticated</description>
<role-name>All Authenticated</role-name>
</security-role>
-->
</auth-constraint>

```

5. Locate the end of the </login-config> element, and add the All Authenticated users role-element after the closing tag.

```

<security-role>
<description>All Authenticated</description>
<role-name>All Authenticated</role-name>
</security-role>

```

6. Search for the first instance of a <security-constraint> tag, and add the following <security-constraint> tag before that tag.

Important: Enter the information below as single lines without line breaks.

```

<security-constraint>
<web-resource-collection>
<web-resource-name>action</web-resource-name>
<description>Define the non-secured resource</description>
<url-pattern>/P8BPMWSBroker/*</url-pattern>
</web-resource-collection>
</security-constraint>

```

7. Save your changes to web.xml and close the file.

Editing web.xml for SSO

You can use SSO with a proxy server in your Application Engine environment. To enable this optional approach, edit the web.xml file on the WebSphere Application Server.

1. Make a backup copy of web.xml.

```
AE_install_path/Workplace/WEB-INF/web.xml
```

2. Open web.xml for editing, search for the parameter challengeProxyEnabled, and set it to false.

```

<param-name>challengeProxyEnabled</param-name>
<param-value> false </param-value>

```

3. Search for the first instance of <web-resource-collection>, and uncomment the <url-pattern> as noted in the file comments.

```

<web-resource-collection>
<web-resource-name>action</web-resource-name>
<description>Define the container secured resource</description>
<url-pattern>/containerSecured/*</url-pattern>

```

```
<!--
```

Uncomment this section if all resources that require credentials must be secured in order to obtain a secured Thread. If using WebSphere, this section must be uncommented. --> Move this commenting tag here from just before the </web-resource-collection> closing tag below.

```

<url-pattern>/containerSecured/*</url-pattern>
<url-pattern>/</url-pattern>
<url-pattern>/author/*</url-pattern>
<url-pattern>/Browse.jsp</url-pattern>
<url-pattern>/eprocess/*</url-pattern>
<url-pattern>/Favorites.jsp</url-pattern>
<url-pattern>/GetPortalSitePreferences.jsp</url-pattern>
<url-pattern>/GetTokenSignIn.jsp</url-pattern>
<url-pattern>/GetUserInformation.jsp</url-pattern>
<url-pattern>/GetUserToken.jsp</url-pattern>
<url-pattern>/HomePage.jsp</url-pattern>
<url-pattern>/IntegrationWebBasedHelp.jsp</url-pattern>
<url-pattern>/is/*</url-pattern>
<url-pattern>/operations/*</url-pattern>
<url-pattern>/properties/*</url-pattern>
<url-pattern>/redirect/*</url-pattern>
<url-pattern>/regions/*</url-pattern>
<url-pattern>/Search.jsp</url-pattern>
<url-pattern>/select/*</url-pattern>
<url-pattern>/SelectReturn.jsp</url-pattern>
<url-pattern>/Tasks.jsp</url-pattern>
<url-pattern>/UI-INF/*</url-pattern>
<url-pattern>/utils/*</url-pattern>
<url-pattern>/WcmAdmin.jsp</url-pattern>
<url-pattern>/WcmAuthor.jsp</url-pattern>
<url-pattern>/WcmBootstrap.jsp</url-pattern>
<url-pattern>/WcmCloseWindow.jsp</url-pattern>
<url-pattern>/WcmDefault.jsp</url-pattern>
<url-pattern>/WcmError.jsp</url-pattern>
<url-pattern>/WcmJavaViewer.jsp</url-pattern>
<url-pattern>/WcmObjectBookmark.jsp</url-pattern>

```

```

<url-pattern>/WcmQueueBookmark.jsp</url-pattern>
<url-pattern>/WcmSignIn.jsp</url-pattern>
<url-pattern>/WcmSitePreferences.jsp</url-pattern>
<url-pattern>/WcmUserPreferences.jsp</url-pattern>
<url-pattern>/WcmWorkflowsBookmark.jsp</url-pattern>
<url-pattern>/wizards/*</url-pattern>
<url-pattern>/Author/*</url-pattern>
<url-pattern>/axis/*.jws</url-pattern>
<url-pattern>/Browse/*</url-pattern>
<url-pattern>/ceTunnel</url-pattern>
<url-pattern>/CheckoutList/*</url-pattern>
<url-pattern>/downloadMultiTransferElement/*</url-pattern>
<url-pattern>/ExternalUrl/*</url-pattern>
<url-pattern>/findRecordTarget</url-pattern>
<url-pattern>/formCallback/*</url-pattern>
<url-pattern>/getAnnotSecurity/*</url-pattern>
<url-pattern>/getCEAnnotations/*</url-pattern>
<url-pattern>/getContent/*</url-pattern>
<url-pattern>/getForm/*</url-pattern>
<url-pattern>/getISAnnotations/*</url-pattern>
<url-pattern>/getISAnnotSecurity/*</url-pattern>
<url-pattern>/getISContent/*</url-pattern>
<url-pattern>/getMultiContent/*</url-pattern>
<url-pattern>/getPreview</url-pattern>
<url-pattern>/getProcessor/*</url-pattern>
<url-pattern>/getRealms/*</url-pattern>
<url-pattern>/getUsersGroups/*</url-pattern>
<url-pattern>/Inbox/*</url-pattern>
<url-pattern>/integrationCommandProxy</url-pattern>
<url-pattern>/integrationResponse</url-pattern>
<url-pattern>/integrationResponseProxy</url-pattern>
<url-pattern>/integrationWebBasedCommand</url-pattern>
<url-pattern>/keepAlive</url-pattern>
<url-pattern>/launch/*</url-pattern>
<url-pattern>/PublicQueue/*</url-pattern>
<url-pattern>/putContent/*</url-pattern>
<url-pattern>/QuickSearch/*</url-pattern>
<url-pattern>/signingServlet/*</url-pattern>
<url-pattern>/transport/*</url-pattern>
<url-pattern>/upload/*</url-pattern>
<url-pattern>/vwsimsoapervlet</url-pattern>
<url-pattern>/vwsoaprouter</url-pattern>
<url-pattern>/Workflows/*</url-pattern>

```

Move the closing comment tag from here to the location indicated at the beginning of this example.

```

</web-resource-collection>

```

4. Locate the section <auth-constraint>, comment the wildcard (*) <role-name> as noted in the file comments.

```

<auth-constraint>
<!-- <role-name>*</role-name> -->
<!-- For WebSphere 6, use
the role-name line below instead of the wildcard role above.
-->

<role-name>All Authenticated</role-name>

<!-- For WebSphere 6, add this
security-role element below the login-config element (below).
<security-role>
<description>All Authenticated</description>
<role-name>All Authenticated</role-name>
</security-role>
-->
</auth-constraint>

```

5. Locate the end of the </login-config> element, and add the All Authenticated users role-element after the closing tag.

```

<security-role>
<description>All Authenticated</description>
<role-name>All Authenticated</role-name>
</security-role>

```

6. Search for the first instance of a <security-constraint> tag, and add the following <security-constraint> tag before that tag.

Important: Enter the information below as single lines without line breaks.

```

<security-constraint>
<web-resource-collection>
<web-resource-name>action</web-resource-name>
<description>Define the non-secured resource</description>
<url-pattern>/P8BPMWSBroker/*</url-pattern>
</web-resource-collection>
</security-constraint>

```

7. At the end of web.xml, comment out the <login-config> element.

```

<!--
<login-config>
<auth-method>FORM</auth-method>
<realm-name>AE Workplace</realm-name>
<form-login-config>
<form-login-page>/ContainerLogin.jsp</form-login-page>
<form-error-page>/ContainerError.jsp</form-error-page>
</form-login-config>
</login-config>
-->

```

8. As needed, set the *ssoProxyContextPath*, *ssoProxyHost*, *ssoProxyPort*, and *ssoProxySSLPort*.

These parameter values are used to modify one or more elements of the native URL that Workplace sees on a request. Wherever the value of an SSO proxy host element in the URL request is different from the equivalent information for the host where Workplace is deployed, you must set the corresponding SSO *<proxy host element>* parameter for that element in the URL to the value for the SSO proxy host.

```

<init-param>
<param-name>ssoProxyContextPath</param-name>
<param-value></param-value>
</init-param>
<init-param>
<param-name>ssoProxyHost</param-name>
<param-value></param-value>
</init-param>
<init-param>
<param-name>ssoProxyPort</param-name>
<param-value></param-value>
</init-param>
<init-param>
<param-name>ssoProxySSLPort</param-name>
<param-value></param-value>
</init-param>

```

In general, the <init-param> parameters must be configured as follows:

ssoProxyContextPath

Set the value to the context path of the SSO proxy host URL. This is the path portion of the URL that appears after the server name, and which represents top-level access to the Workplace application.

For example, if the Workplace deployment host URL is `http://deploy_server:2809/Workplace` and the SSO proxy host URL is `http://sso_proxy_server.domain.com/fn/Workplace`, then use the following setting:


```
<param-name>ssoProxyContextPath</param-name>
<param-value>/Workplace</param-value>
```

ssoProxyHost

Set the value to the SSO proxy host server name. Typically, this is a full domain-qualified host name.

For example, if the host URL where Workplace is deployed is `http://deploy_server/Workplace` and the corresponding SSO proxy host URL is `http://sso_proxy_server/Workplace`, then use the following setting:

```
<param-name>ssoProxyHost</param-name>
<param-value>sso_proxy_server</param-value>
```

ssoProxyPort

Set the value to the http port on the SSO proxy host.

For example:

```
<param-name>ssoProxyPort</param-name>
<param-value>80</param-value>
```

ssoProxySSLPort

Set the value to the https port on the SSO proxy host, if defined or used to access Workplace pages.

For example:

```
<param-name>ssoProxySSLPort</param-name>
<param-value>443</param-value>
```

9. Save your changes to `web.xml` and close the file.

Configuring Java Virtual Machine settings for JAAS login and memory

Use the Java Virtual Machine settings in the WebSphere Application Server to set up JAAS login information for authentication and memory settings for resource usage.

Remember: In high availability clustered server configurations, for steps that require Java Virtual Machine (JVM) settings to be made make sure to make these changes for every node in the application server configuration.

1. Log in to the WebSphere administrative console.
2. Navigate to the Java Virtual Machine settings at **Servers > Server Types > WebSphere application servers > server_name > Java & Process Management > Process Definition > Java Virtual Machine**.
3. In the **Generic JVM arguments** field, add the following entry:

```
-Djava.security.auth.login.config=AE_install_path
\CE_API\config\jaas.conf.WebSphere
```

Replace *AE_install_path* in the entry above with your actual installation path, for example:

AIX, HPUX, Linux, Linux on System z, Solaris:

```
-Djava.security.auth.login.config=opt/FileNet/AE
/CE_API/config/jaas.conf.WebSphere
```

Windows:

```
-Djava.security.auth.login.config=C:\Progra~1\FileNet\AE
\CE_API\config\jaas.conf.WebSphere
```

Windows 64-bit server with Application Engine installed in the Program Files (x86) directory:

```
-Djava.security.auth.login.config=C:\Progra~2\FileNet\AE  
\CE_API\config\jaas.conf.WebSphere
```

Your path might be slightly different based on the version of your client installations, or whether you have chosen a custom path for the installation. Verify the location of this file and specify the install path location before you enter the path.

Important: Do not copy and paste the text from this guide into the field in the console because hidden formatting can cause problems with the entry. Use a paste special option in a text editor to remove formatting first, or type the entry into the field.

4. Set the Initial heap size and Maximum heap size, and save your changes.

For example, you might set the Initial heap size to 512 and the Maximum heap size to 1024. However, these values vary significantly depending on your machine size.

Refer to your application server vendor recommendation for Initial heap size and Maximum heap size values. For IBM specific recommendations, see the *IBM FileNet P8 Performance Tuning Guide*.

5. (For installations with Content Platform Engine and Application Engine collocated on the WebSphere server, but in different WebSphere profiles) Create an additional JVM property for different WebSphere profiles.


Perform the following steps on both the Content Platform Engine profile and the Application Engine profile:

- a. In the Java Virtual Machine settings, create a Custom Property:

```
com.ibm.websphere.orb.uniqueServerName
```

- b. Set the **Value** to true.
- c. Save your changes.
- d. Restart WebSphere Application Server.

Related information:

 Product documentation for IBM FileNet P8 Platform
Download the IBM FileNet P8 Platform documentation.

Configuring Lightweight Third Party Authentication (LTPA)

To set up LTPA security, configure settings to match on both the Content Platform Engine application server and the Application Engine application server. If your Application Engine and Content Platform Engine are on the same WebSphere Application Server, you are not required to configure LTPA.

Note: If your environment uses Workplace XT, follow the instructions for configuring Light weight Third Party Authentication (LTPA) in the *IBM FileNet Workplace XT Installation and Upgrade Guide*.

Important: In a highly available WebSphere environment where Content Platform Engine and Application Engine are managed by different deployment managers, perform any LTPA configuration steps on the administrative server only. The scope of this action will affect the entire application server configuration.

If you are already using LTPA with your Content Platform Engine application server, you must export only the existing keys and copy the key file to the Application Engine server. Check with your Content Platform Engine administrator.

To configure LTPA:

1. On the Content Platform Engine server, log in to the WebSphere administrative console.
2. Navigate to the LTPA settings page at **Security > Global security** and select **LTPA** from the right side of the panel.
3. Enter a value for the **LTPA timeout** that is larger than the default. For example, if the timeout value is left at the default value of 120 minutes, the LTPA key expires after 2 hours. Users will not be able to log in to Workplace after being logged in for 2 hours.

Important: In high availability environments, set the timeout value for forwarded credentials between servers:

Option	Description
WebSphere Application Server 7.0	60000

4. Save your changes.
 5. In the box for **Cross-cell single sign-on**, type a password to create the **LTPA password**.
For password restrictions, see the WebSphere Application Server documentation. If you have already configured Content Platform Engine for LTPA, use the existing password in the Application Engine configuration.
 6. Enter the fully qualified path for the **Key File Name**. For example, `/opt/LTPA/ltpa_key_name`.
 7. Click **Export keys**. Verify that a message like the following message is displayed: The keys were successfully exported to the file `ltpa_key_name`.
 8. Click **OK**, then click **Save changes directly to the master configuration**.
 9. Stop and restart the WebSphere Application Server instance.
 10. Copy the key file from the Content Platform Engine server location you specified to a directory on the Application Engine server. For example, `/opt/LTPA/ltpa_key_name`
 11. On the Application Engine server, log in to the WebSphere administrative console.
 12. Navigate to the LTPA settings page at **Security > Global security** and select **LTPA** from the right side of the panel.
 13. Enter a value for the **LTPA timeout** that is larger than the default. For example, if the timeout value is left at the default value of 120 minutes, the LTPA key expires after 2 hours. Users will not be able to log in to Workplace after being logged in for 2 hours.
- Note:** In high availability environments, set the timeout to 60,000.
14. Save your changes.
 15. In the box for **Cross-cell single sign-on**, type and confirm the **LTPA password** you created for Content Platform Engine.
For password restrictions, see the WebSphere Application Server documentation. If you have already configured Content Platform Engine for LTPA, use the existing password in the Application Engine configuration.
 16. Specify the path for the key file that you copied to the Application Engine server. For example, `/opt/LTPA/ltpa_key_name`.
 17. Click **Import keys**. Verify that a message like the following one is displayed: The keys were successfully imported from the file `ltpa_key_name`.
 18. Save your changes.

In a highly available environment, synchronize the changes across all nodes after saving your configuration settings.

Related tasks:

Starting or stopping an application server instance

Related information:



Configuring LTPA for Workplace XT on WebSphere Application Server

To set up LTPA security, you must configure settings to match on both the Content Engine Web application server and the Workplace XT Web application server. If your Workplace XT and Content Engine are on the same WebSphere Application Server, you do not need to configure LTPA.

Configuring stand-alone Lightweight Directory Access Protocol (LDAP)

To enable LDAP communication between Application Engine and Content Engine, you must configure settings on the WebSphere Application Server. It is recommended that the LDAP configuration settings match those set on the application server where Content Engine is installed.

Important: If you are using WebSphere Application Server Network Deployment and Application Engine is to be deployed where Content Platform Engine is deployed, you do not need to complete this task because you already configured LDAP as part of configuring Content Platform Engine.

To configure stand-alone Lightweight Directory Access Protocol (LDAP):

1. Open the WebSphere administrative console.
2. Navigate to the security settings page at **Security > Global security**.
3. Disable security by using the following Security settings:
 - Disable (clear) the **Enable Administrative Security** flag.
 - Disable (clear) the **Enable application security** flag.
 - Disable (clear) the **Java 2 security** flag.
4. From the bottom of the panel, in the dropdown list called **Available realm definitions**, select **Standalone LDAP registry** and click **Configure**.
5. Configure the LDAP provider to exactly match the corresponding settings on the Content Engine application server.

Tip: Open the WebSphere administrative console for Content Engine to the same panels to see and copy all settings.

- Primary administrative user name
 - Select Automatically generated server identity.
 - Type
 - Host
 - Port
 - Base distinguished name (DN)
 - Bind distinguished name (DN)
 - Bind password
6. Configure the LDAP user registry settings to exactly match the corresponding settings on the Content Engine application server.

Tip: Open the WebSphere administrative console for Content Engine to the same panel to see and copy all settings.

- User filter
 - Group filter
 - User ID map
 - Group member ID map
 - Certificate map mode
 - Certificate filter
7. Save these settings.
 8. Next to **Available realm definitions**, ensure that **Standalone LDAP registry** is still selected, and click **Set as current**.
 9. Set the following Security flags:
 - Enable (select) the **Enable Administrative Security** flag.
 - Enable (select) the **Enable application security** flag.
 - Disable (clear) the **Java 2 security** flag.

The IBM FileNet P8 Platform utilizes LDAP-based security, and does not support Java 2 security. Enabling Java 2 security will cause unexpected behavior.
 10. Save your changes to the master configuration.
 11. Restart the WebSphere instance.
 12. Test the connection on the Standalone LDAP registry page. If the test fails, correct the error before proceeding. If it passes, click **OK** to return to the previous page.

Configuring Lightweight Directory Access Protocol (LDAP) for federated repositories

If you have a multiple domain environment, configure LDAP settings for federated repositories on the WebSphere Application Server to enable LDAP communication between Application Engine and Content Engine. It is recommended that the LDAP configuration settings match those set on the application server where Content Engine is installed.

Important: If you are using federated repositories, your WebSphere administrative console user cannot have the same username or ID as a user in the LDAP repository.

Important: If you are using WebSphere Application Server Network Deployment and Application Engine is to be deployed where Content Engine is deployed, you do not need to complete this task.

To configure Lightweight Directory Access Protocol (LDAP) for federated repositories:

1. Open the WebSphere administrative console.
2. Navigate to the security settings page at **Security > Global security**.
3. Set the following Security flags:
 - Disable (clear) the **Enable Administrative Security** flag.
 - Disable (clear) the **Enable application security** flag.
 - Disable (clear) the **Java 2 security** flag.
4. From the bottom of the panel, in the dropdown list called **Available realm definitions**, select **Federated Repositories** and click **Configure**.
5. Configure the LDAP provider to exactly match the corresponding **General Properties** on the Content Engine application server.

Tip: Open the WebSphere administrative console for Content Engine to the same panels to see and copy all settings.

- Realm name
 - Primary administrative user name
 - Select Automatically generated server identity.
 - Ignore case for authorization
 - Repositories in the realm
6. Save these settings.
 7. Next to **Available realm definitions**, ensure that **Federated repositories** is still selected, and click **Set as current**.
 8. Set the following Security flags:
 - Enable (select) the **Enable Administrative Security** flag.
 - Enable (select) the **Enable application security** flag.
 - Disable (clear) the **Java 2 security** flag.
- The IBM FileNet P8 Platform utilizes LDAP-based security, and does not support Java 2 security. Enabling Java 2 security causes unexpected behavior.
9. Save your changes to the master configuration.
 10. Restart the WebSphere instance.
 11. Test the connection to the repository.
 - a. In the WebSphere administrative console, navigate to **Users and Groups > Manage Users**.
 - b. Click **Search By User ID**, and enter a known user.
 - c. Click **Search**. This should return the user from the configured LDAP repository.

Related tasks:

Starting or stopping an application server instance

Deploying Application Engine on the application server

After you install and configure Application Engine, you must deploy your client application, Workplace, on your application server. You might be required to re-create the WAR or WAR and EAR files before you deploy.

Important: In a high availability environment, for steps that require Java Virtual Machine (JVM) settings to be made make sure to make these changes for every node in the application server configuration:

- web.xml file

If you need to edit the web.xml file as part of deployment, for example if you are using single sign-on (SSO), make these changes from the administrative server node only. In addition, to include these changes you must recreate the WAR or EAR file before deploying the application.

Most application server cluster configurations deploy an application to managed servers by copying the application files from the administrative node to the managed server, and only changes made on the administrative node are deployed to the configuration.

Tip: An additional method for deploying applications to an application server cluster is to maintain a copy of the application on all servers as in a farm of independent servers instead of copying files. In this type of configuration, edits to files should be performed on all nodes in the application server cluster.

- (WebSphere Application Server and WebLogic Server) When installing Application Engine through the administrative server make sure to deploy Application Engine to the cluster of server instances:

Table 26. Deployment actions

Server	Action
WebSphere Application Server	<p>For WebSphere make sure you select the cluster and/or managed nodes that will be running the application when mapping modules to servers (the admin node is usually the default, so it is typical to change this). Click apply so that the application shows as deployed to the proper nodes instead of the default single node.</p> <p>UTF-8 encoding parameters should be set on every node.</p>

- (Farm of independent application server instances) Configure and deploy the Application Engine on each node.

When installing in farm of independent application server instances, the steps shown for deploying Application Engine on the application server must be performed on every node.

Important: Since there is no central administration server every server acts as a separate server instance and must be configured as such.

“Deploying Application Engine on WebSphere Application Server”

After you install and configure Application Engine, you must deploy your client application, Workplace, on your WebSphere Application Server. You might be required to re-create the WAR or WAR and EAR files before you deploy.

Deploying Application Engine on WebSphere Application Server

After you install and configure Application Engine, you must deploy your client application, Workplace, on your WebSphere Application Server. You might be required to re-create the WAR or WAR and EAR files before you deploy.

Remember: In farm and cluster environments, deploy Application Engine on WebSphere Application Server on all nodes.

“Re-creating the WAR or EAR file”

Any time that you change files in the /Workplace directory, such as changes to web.xml for container-managed authentication, SSO support, or any other edits, you must re-create the WAR or EAR file and redeploy your changes.

“Deploying the application (WebSphere Application Server)” on page 105

To use Workplace as a web application, you must deploy it as an application in the WebSphere administrative console. You can specify the context root for the application URL during the deployment.

Re-creating the WAR or EAR file

Any time that you change files in the /Workplace directory, such as changes to web.xml for container-managed authentication, SSO support, or any other edits, you must re-create the WAR or EAR file and redeploy your changes.

Remember: Before re-creating the EAR file, you must first re-create the WAR file.

To re-create the WAR or EAR files:

1. Verify that all modified /Workplace directory files have been saved.
2. Re-create the app_engine.war file by running the script for your platform.

Option	Description
AIX, HPUX, Linux, Linux on System z, Solaris	<i>AE_install_path</i> /deploy/ create_app_engine_war.sh

3. (For WAR file deployment) Rename the newly re-created app_engine.war file to Workplace.war or *custom_name.war* to create the context root for your application. For example, the default app_engine.war generates the following context root: `http://server_name:port#/app_engine`. Renaming the WAR file Workplace.war generates the following context root: `http://server_name:port#/Workplace`.

Important: You must rename the WAR file every time you regenerate it. The create_app_engine_war script creates by default a file with the name app_engine.war.

Important: Do not rename the WAR file if you are using the WAR file to re-create the EAR file for deployment.

4. (For EAR file deployments only) Re-create the app_engine.ear file by running the script for your platform.

Option	Description
AIX, HPUX, Linux, Linux on System z, Solaris	<i>AE_install_path</i> /deploy/ create_app_engine_ear.sh

Deploying the application (WebSphere Application Server)

To use Workplace as a web application, you must deploy it as an application in the WebSphere administrative console. You can specify the context root for the application URL during the deployment.

To deploy Application Engine (Workplace):

1. Log on to the WebSphere administrative console.
2. Navigate to **Applications > WebSphere Enterprise Applications > New Enterprise Applications > Install**.
3. Select the file to deploy.
 - (If the administrative console is running *locally*) Select **Local file system** and enter or browse to the location of the app_engine.war or app_engine.ear file created by the installation program. For example, *AE_install_path*/deploy/app_engine.war or *AE_install_path*/deploy/app_engine.ear. Do not enter the machine name.
 - (If the administrative console is *remote*) Select **Remote file system** and enter the fully qualified path name to the app_engine.war or app_engine.ear file. For example, *AE_install_path*/deploy/app_engine.war or *AE_install_path*/deploy/app_engine.ear. Do not enter the machine name.
4. If you are deploying a WAR file, enter the context root.
Enter Workplace and click **Next** to proceed to deploying a new application.

Tip: The context root is the name of the application you log on to using the web interface, such as: `http://ApplicationEngineServerName:port#/Context_Root`.

5. Click **Prompt only when additional information is required**, and click **Next**. Complete the dialogs for installing a new application, using the following settings:

For **Application name**, enter Workplace, or the name you chose to call the application.

For **WebServer**, specify the server you are planning to use. Verify that your application name is selected and associated with the correct WebServer.

For **Map virtual hosts for Web modules**, for virtual host, choose the default_host.

(WAR file deployment only) For **Context root**, specify Workplace, or whatever you want to call the application.

6. Save your configuration.
7. Navigate to **Applications > Enterprise Applications > Workplace > Class loading and update detection**.
8. Set the polling interval for updated files with a number appropriate for your environment, for example, 3 seconds.
9. Change the **Class loader order** to **Classes loaded with local class loader first (parent last)**.
10. Click **Apply**.
11. Click **Workplace > Manage Modules**.
12. In the **Modules** column, click **Workplace**.
13. Change the **Class loader order** to **Classes loaded with local class loader first (parent last)**.

Important: Change this setting only for the specific web application. Do not change the similar settings for the entire application server.

14. If you are using container-managed authentication, navigate to **Enterprise Applications > Workplace > Security role to user/group mapping**.
 - a. Select the **All Authenticated** role and click **Map Special Subjects**.
 - b. Map the **All Authenticated** role and to **All Authenticated in Applications realm**.
15. Save all your changes to the master configuration.
16. Stop and restart the WebSphere Application Server instance where the application is installed.

To troubleshoot the deployment, check the following log:

```
WAS_install_path/AppServer/profiles/profile_name/logs/server_name/SystemOut.log
```
17. Start Workplace (or whatever you named your application) from the administrative console.
18. In a high availability environment, by using the application server administration tool, verify that the Application Engine application is running.
 - a. Open a web browser and type in the URL for the Application Engine application.
 - If you are using a load-balancer or proxy server the URL has the form:

Application Engine

`http://virtual_name:port_number/Workplace`

- If connecting to an individual cluster node the URL would have the form:

Application Engine

`http://clustered_server_name:port_number/Workplace/`

Sign-in by using the virtual name to properly set the base Application Engine URL. If it is not set correctly you must change it in Site Preferences.

- Verify that the sign-in page displays, and log in as a user.
- Fail one of the nodes.
- Verify that you can reload the sign-in page, and log in as the same user.

Related tasks:

Starting or stopping an application server instance

Setting Application Engine bootstrap preferences

By successfully signing in to Workplace and saving the bootstrap preferences, you verify basic Application Engine functionality such as user authentication as well as communication and storing of data in Content Engine.

“Setting the bootstrap properties on first login”

Six bootstrap preference groups are available for configuring the first time you sign in to Workplace.

“Verifying that a single index has been added for Application Name on the site preferences object store” on page 110

To properly index access roles and improve login performance on Application Engine, an index is created for Application Name on the object store that contains the Workplace site preferences. You can verify this index setting after you have successfully configured the bootstrap preferences.

“Enabling user access to the workflow subscription wizard” on page 110

To allow users to create workflows subscriptions, you must configure the PWDesigner access role using the Workplace Site Preferences, and give the users appropriate access rights to the workflow subscriptions classes.

“Enhanced Timezone Detection” on page 111

You can set the **useEnhancedTimeZoneDetection** parameter to accurately detect a time zone for a client browser. This setting cannot be modified through the Site Preferences page. To enable this feature you must manually modify the `bootstrap.properties` file.

Setting the bootstrap properties on first login

Six bootstrap preference groups are available for configuring the first time you sign in to Workplace.

In addition to the preferences covered in this topic, more preferences can be set for the Workplace application by using Workplace Site Preferences. For more information, see the IBM FileNet P8 help topic **Working with documents and other content > Working with documents in Workplace XT > Site preferences**.

- Log on to Workplace:
 - On any computer, open a browser and type:
`http://ApplicationEngineServerName:port#/Workplace`

Important: *ApplicationEngineServerName* cannot be localhost or an IP address.

- b. Enter a user name and password, and then click **Sign in**. The Bootstrap Preferences page opens.

The user who initially logs in and sets the bootstrap preferences is automatically added to the Application Engine Administrators role. For more information, see the IBM FileNet P8 help topic **Working with documents and other content > Working with documents with Workplace XT > Site preferences > Access roles preferences**.

2. Enter security info (required for SSL only).

- a. Enter the SSL Host and Port information for the SSL server.
 - b. Enter the Java Server HTTP port.

Use the Security info preference to redirect sign-ins through a Secure Socket Layer (SSL) server and to identify a remote Java server. This encrypts the user IDs and passwords when they travel over the network. See “Setting up Application Engine SSL security” on page 117 for instructions on setting up SSL security for one or more Application Engine installations.

Important: After you have configured SSL, the Site Preferences application also runs under SSL to protect the guest account's user ID and password. This means that when you run Site Preferences on an unsecured server that redirects sign-ins to an SSL server, you will be editing the Bootstrap preferences of the SSL server (stored in the `bootstrap.properties` file). This does not affect the General, Object Store, and Shortcut preferences, which are retrieved from the preferences file saved in the object store.

3. Configure user token settings.

User Tokens are used by IBM FileNet P8 applications to launch into each other without the need for an additional login.

- a. Select whether or not to create user tokens for your Application Engine (Default: Yes).
 - b. Select whether or not the application will pick up generated tokens from other applications (Default: Yes).
 - c. Specify a Token timeout interval (1 - 15 minutes).

4. (Required) Specify preference settings.

Preference settings specify the name of the site preference file, its storage location (object store), and the documentation server URL. The site preferences file is checked into the object store the first time you log on to Workplace. The site preferences are stored as XML data in this file, *Site Preferences for Preferences name.xml*. Use Enterprise Manager to access this file, and navigate to **Object Stores > Object Store location > Root Folder > Preferences**.

The bootstrap preferences are saved in the `bootstrap.properties` file, and not in the site preferences file. The default location for this file is `AE_install_path/FileNet/Config/AE`.

- a. Select an object store from the **Object store location** choice list. The preferences file will be saved in this object store. Workplace users must have access to this object store.
 - b. Enter a preference file name in the **Preferences name** field.
 - c. Enter the base documentation server URL in the **Documentation server** field.

The format of the base documentation URL depends on the documentation package you use:

Table 27. Base documentation URLs

FileNet P8 documentation package	URL
Online information center at www.ibm.com	http://pic.dhe.ibm.com/infocenter/p8docs/v5r2m0/topic/com.ibm.p8.doc
Installed P8 information center	http://server_name:port#/application_name/topic/com.ibm.p8.doc where: <ul style="list-style-type: none"> • <i>server_name</i> is the name of the server where the FileNet P8 Platform documentation information center is installed. • <i>port#</i> is the port number. • <i>application_name</i> is the name of the deployed FileNet P8 Platform application. If you installed a local information center, the application name is typically p8docs

If no documentation URL is specified, the Workplace Help link defaults to <http://localhost>.

- d. Enter the ISRA Interface Servlet URL.

For more information, see “Enabling Application Engine to use ISRA” on page 130.

5. Set Banner Image.

The banner image is the graphic that appears at the upper left-hand side of the Workplace application pages. If you have a banner image that you would like to use in place of the default, follow this procedure.

- a. Copy the new graphic file to the location of your choice on Application Engine in the /FileNet/AE/Workplace folder.
- b. In the Path field, type the path (relative to the /Workplace folder) to the new banner graphic file.
- c. In the Image Width field, type the width of the image (in pixels).
- d. In the Image Height field, type the height of the image (in pixels).

6. Configure Application Integration.

This preference setting only affects Outlook integration.

Select No (default) if you do not want users to be prompted to add an e-mail to an object store each time the e-mail is sent.

Select Yes if you want users prompted to add an e-mail to an object store when the e-mail is sent.

7. Add Application Engine Administrators (*ae_admin_user*). Add the users and groups that will perform Application Engine administration tasks to the Application Engine Administrators role.

The user who initially signs in and sets the bootstrap preferences is automatically added to the Application Engine Administrators role. For more information, see the IBM FileNet P8 help topic **Working with documents and other content > Working with documents with Workplace XT > Site preferences > Access Roles preferences**.

To modify the access roles after the initial bootstrap configuration, users with the Application Engine Administrators role can use the access roles section of the Workplace Site Preferences. Launch Workplace and navigate to **Admin > Site Preferences > Access Roles**.

When you access the bootstrap preference page via the Site Preferences application, an additional preference, **Guest info** (to allow guest sign ins), is also available.

8. Click **Apply** to save your bootstrap settings.

After the initial bootstrap configuration, users with the Application Engine Administrators (*ae_admin_user*) role can change any of these preferences by signing into Workplace and navigating to **Admin > Site Preferences > Bootstrap**.

In a web farm/clustered environment, all Application Engine installations share site preferences by using the same bootstrap.properties file.

Verifying that a single index has been added for Application Name on the site preferences object store

To properly index access roles and improve login performance on Application Engine, an index is created for Application Name on the object store that contains the Workplace site preferences. You can verify this index setting after you have successfully configured the bootstrap preferences.

To verify the index setting:

1. On Content Engine, launch the Enterprise Manager.
2. In the left pane, expand the **Object Stores** folder.
3. Expand the object store node where your site preferences are stored.
4. Expand **Other Classes** and then **Custom Object**.
5. Right click **Access Role** and select **Properties**.
6. Select the **Property Definitions** tab.
7. Select **Application Name** and click **Edit**.
8. On the General tab of the Application Name Properties, verify that the **Indexed** field shows Single Indexed.
 - If the **Indexed** field shows Single Indexed, click **OK**. The verification is complete. Skip the remaining steps in this procedure.
 - If the **Indexed** field shows Not indexed, continue with the following steps to change the setting.
9. Click **Set/Remove**.
10. Select **Set** and then **Single Indexed**.
11. Click **OK** to set the index.
12. Click **OK** to apply the change and close the Application Name Properties window.
13. Click **OK** to close the Access Role Class Properties window.

Enabling user access to the workflow subscription wizard

To allow users to create workflows subscriptions, you must configure the PWDesigner access role using the Workplace Site Preferences, and give the users appropriate access rights to the workflow subscriptions classes.

1. Assign users as members of the PWDesigner access role. See the FileNet P8 help topic **Working with documents and other content > Working with documents with Workplace XT > Site preferences > Access roles preferences** .

2. Run the security script wizard with the `workplacescript.xml` file to add accounts to the Workflow Designer role. In Enterprise Manager, right-click the domain root node or the object store node and select **All tasks > Run Security Script Wizard**.

For more information about how to use the Security Script wizard to assign the Workflow Designer role to user or group accounts, and more information about the `workplacescript.xml` file and how roles are defined in the Enterprise Manager, see the FileNet P8 help topic **Administering FileNet P8 > Administering Content Platform Engine > Defining the repository infrastructure > Managing security > Security script wizard**.

Enhanced Timezone Detection

You can set the **useEnhancedTimeZoneDetection** parameter to accurately detect a time zone for a client browser. This setting cannot be modified through the Site Preferences page. To enable this feature you must manually modify the `bootstrap.properties` file.

For more information, see the IBM FileNet P8 help topic **Administering IBM FileNet P8 > Administering Application Engine > Application Engine Administration**.

Updating Application Engine settings in a load balanced environment

You can update Application Engine settings in a load balanced Application Engine environment consisting of a load balancer or proxy device, several HTTP servers and several application server instances.

When several application server instances host the Application Engine application the goal is to provide to end-users the same work environment from every server instance. Application Engine utilizes a number of preference settings and configuration information to customize the Application Engine application for user needs. In order to provide a seamless work experience in an environment with multiple application server instances residing behind a load-balancer or proxy device it is important that each instance access the same configuration data.

The installer allows you to select the location of a shared configuration directory during the installation process. This shared configuration directory is used to store the files that contain preference settings and configuration information for the Application Engine application. A shared configuration directory allows you to have a single Application Engine instance with the same configuration information and preferences across multiple server instances. The process for managing settings by using a shared configuration directory is documented later in this section.

The shared configuration directory should ideally be placed on a highly available share or NFS exported directory that is accessible by all systems in the application server configuration.

Important: To be able to perform these tasks you must be a user assigned the Application Engine Administrator access role, and have copy/overwrite permissions on the directories shown later in this section on all nodes.

If you need to update your Application Engine Site Preferences you must refresh the configuration files on each node server.

To update Application Engine settings in a load balanced environment:

1. Make your Application Engine configuration changes.
 - a. Sign into Application Engine as a user who is assigned the Application Engine Administrator access role.

Application Engine:
`http://virtual_name:port_number/Workplace`
 - b. Click **Admin**.
 - c. Click **Site Preferences**.
 - d. Update your settings.
 - e. Click **Exit**.
2. Reload the Application Engine configuration files on each node.

After changes are made you must reload the Application Engine configuration files on each node server.

To load identical settings on all the nodes you must perform the following steps on each individual node server by logging in to the Application Engine instance running on the server.

Restriction: Do not log in by using the load balancer URL.

 - a. Sign into Application Engine as a user who is assigned the Application Engine Administrator access role.
 - b. Use the following URL to sign in:

Application Engine:
`http://node_server_name:port#/Workplace`
 - c. Click **Admin**.
 - d. Click **Site Preferences**.
 - e. Click **Refresh**.
 - f. From the Refresh page, click **Reload configuration files**.
 - g. Click **Exit**.

For more information and a list of all configuration files that can be reloaded, go to the on-line help and navigate to:

Application Engine:

Developer Help > Workplace Development > Workplace Customization Guide > Appendixes > Reloading Workplace Configuration Files

Configuration and startup tasks

After you install the FileNet P8 components, there are some additional steps to configure the system. After you configure the FileNet P8 components, familiarize yourself with system startup and shutdown procedures. See the **Administering FileNet P8 > Starting and stopping FileNet P8 components** help topic.

“Configuring the workflow system connection point for Application Engine”
Before users can access workflow tasks and work items from Workplace, you must configure the connection point on the Application Engine.

“Setting up Content Platform Engine and client transport SSL security” on page 114

Configuring SSL enables secure communications between the Content Platform Engine and the directory service, as well as between Content Platform Engine clients and the Content Platform Engine server.

“Setting up Application Engine SSL security” on page 117

You can configure an Application Engine to direct sign-ins through a Secure Socket Layer (SSL) https connection. This configuration takes place after you have installed and configured Application Engine.

“Performing additional configuration tasks” on page 120

After you have completed the installation tasks, your core FileNet P8 system is operational. You can do the recommended additional configuration tasks to prepare the system for general use.

Configuring the workflow system connection point for Application Engine

Before users can access workflow tasks and work items from Workplace, you must configure the connection point on the Application Engine.

Make sure that you have already created a region and a connection point and that the Content Platform Engine software is running.

To configure the connection point:

1. Sign in to Workplace as an Application Engine Administrator:
 - a. On any computer, open a browser and navigate to:
`http://ApplicationEngineServerName:port#/Workplace`
 - b. Sign in with the same account that you used to set the bootstrap preferences.
2. Click **Admin**.
3. Click **Site Preferences**.
4. Under **General Settings > Tasks**, select a **Process Engine Connection Point** from the list.
5. Click **Apply**.
6. Click **Exit**.

Important: Initializing the isolated region, as described in the next step, in an existing environment will destroy all data in the existing region.

7. (For new installations only) Initialize the isolated region. If you initialized the isolated region earlier, do not initialize it again.

- a. Click **Admin**.
- b. Click **Process Configuration Console**.
If your computer does not have the appropriate Java Runtime Environment (JRE) installed, you will be prompted to download the JRE at this point; follow the prompts to complete the download. During the installation process, click the **Browser** tab and clear the **Internet Explorer** option.
- c. Right-click the icon or **name of the isolated region** you want to initialize, and select **Connect**.
- d. Click **Action**.
- e. Click **Initialize Isolated Region**.
- f. Click **Yes** at the prompt asking if you want to continue.
- g. Close the Process Configuration Console.
8. In Workplace, click **Tasks** to confirm that Application Engine is communicating with Process Engine.
9. Sign out of Workplace.

Setting up Content Platform Engine and client transport SSL security

Configuring SSL enables secure communications between the Content Platform Engine and the directory service, as well as between Content Platform Engine clients and the Content Platform Engine server.

Important: It is a best practice to enable SSL for the Content Platform Engine web services. Authentication over these two web services is usually performed by providing username and password credentials. If these web services are not configured to run over an SSL connection, clear text passwords will be sent across the network. (However, this is not true when Kerberos-based authentication is used. Kerberos authentication is available only for the Content Platform Engine web service.) The option not to use SSL over these two web services is provided primarily for development systems or other non-production systems where the security provided by SSL might not be required.

For access to the Content Platform Engine through the EJB transport (IIOP or T3 protocol), an SSL connection is necessary to provide privacy for data sent across the network. However, user passwords would not be compromised if SSL were not used. While it is preferable to use SSL with the EJB transport (IIOP or T3 protocol), it is not a requirement.

- The Content Platform Engine web service is used:
 - By all clients of the Content Platform Engine .NET API
 - By all clients of the Content Platform Engine COM Compatibility API (CCL)
 - By Enterprise Manager tool and FileNet Deployment Manager tools
 - By the Component Manager
- Certain Java applications (written against the Content Platform Engine zJava API) might use the Content Platform Engine web service transport, but typically they would use EJB transport (IIOP or T3 protocol).
- The Application Engine server uses only the EJB transport to communicate with the Content Platform Engine.

“Enabling SSL for Content Platform Engine” on page 115

When you enable SSL, a server certificate is added to the Directory Services server (for authentication). In addition, the CA certificate is added in two

different locations on the Content Platform Engine server (the JDK path location is for authorization). Take care to ensure that the proper certificate is added to each of the three locations.

“Enabling SSL between Enterprise Manager and the directory service” on page 117

Use the Enterprise Manager interface to enable SSL between Enterprise Manager and the directory service.

“Enabling SSL between IBM Administration Console for Content Platform Engine and the directory service” on page 117

You need to enable SSL between IBM Administration Console for Content Platform Engine and the directory service.

Enabling SSL for Content Platform Engine

When you enable SSL, a server certificate is added to the Directory Services server (for authentication). In addition, the CA certificate is added in two different locations on the Content Platform Engine server (the JDK path location is for authorization). Take care to ensure that the proper certificate is added to each of the three locations.

To enable SSL for Content Platform Engine:

1. Obtain and install a server certificate and a CA certificate on the directory service. These certificates are available from independent certificate authorities, such as VeriSign, or you can generate your own certificates if you have the necessary certificate management software installed.
2. Enable SSL on the directory service and set the SSL port number. The default SSL port number is 636; however, if you have more than one directory service that is using SSL on the server, you might need to use a non-default port number. See your directory server documentation for instructions.
3. On the Content Platform Engine server, add the CA certificate to the application server keystore, if it does not already contain it.
4. On the Content Platform Engine server, add the CA certificate to the JDK (Java) keystore, if it does not already contain it. You can use the default key store, or create your own key store in a custom location.
 - To use the JDK default Java key store, do the following:
 - a. Determine the Java version your application server uses and the JAVA_HOME location.
 - b. Use the keytool to import the CA certificate to the Java keystore at %JAVA_HOME%\jre\lib\security\cacerts.
 - c. To improve security, change the default password.
 - To use your own key store (rather than the JDK default key store), do the following:
 - a. Add the following system parameters to the Java command line in your application server startup script:

```
-Djavax.net.ssl.trustStore= path_to_your_keystore_file
-Djavax.net.ssl.trustStorePassword= password_of_your_keystore
```
 - b. Use the Java keytool to import the CA certificate to your own keystore.
5. Start IBM Administration Console for Content Platform Engine if you did not already do so:
 - a. On any computer, open a browser and navigate to `http://CPE_Server:port/acce`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.

- b. Log on as the `gcd_admin` user.
6. Use IBM Administration Console for Content Platform Engine to set the port number to match the SSL port number on the directory server:
 - a. Select the domain node in the navigation pane.
 - b. Select **Properties** in the details pane, open the drop-down list for Directory Configurations, and select your directory server type.
 - c. Set the Directory Server Port value to match the SSL port on the directory server.
 - d. Click **Close**.
7. Obtain another server and CA certificate for the Content Platform Engine.
8. Create a custom identity keystore on the Content Platform Engine server, and add the server certificate to the custom keystore.
9. Using the application server administration tool, enable SSL and point to the custom identity keystore. Directions vary by application server type; see your application server documentation for detailed procedures.

Option	Description
WebSphere Application Server	Configure an SSL repertoire. In the left pane of the WebSphere administrative console, navigate to Security > SSL. In the right pane, select your Java Secure Socket Extension (JSSE) repertoire and specify key and trust file names and passwords.

10. Configure clients to use a particular URL for connecting to Content Platform Engine based on the application server type and the client transport (protocol) type. The following table provides the default ports and sample URLs:

Table 28. Default ports and sample URLs

Protocol	SSL	Default Port	App Server	Sample URL
HTTP	no	9080	WebSphere Application Server	<code>http://mycorp.com:9080/wsi/FNCEWS40MTOM/</code>
HTTPS	yes	9443	WebSphere Application Server	<code>https://mycorp.com:9443/wsi/FNCEWS40MTOM/</code>
IIOP	no	2809	WebSphere Application Server	<code>iiop://mycorp.com:2809/FileNetEngine</code>
IIOP	yes	2809	WebSphere Application Server	<code>iiop://mycorp.com:2809/FileNetEngine (default)</code>

While the default port for IIOP with SSL is port 9403, use port 2809. The web application server resolves the SSL port number correctly.

The port values in the table are default values. If you change the port that your application server listens on, you might need to change the port number used by the Content Platform Engine client.

11. (Oracle WebLogic Server on AIX, HP-UX, Linux, Linux on System z, Solaris) Regardless of the JRE version that you used when you installed Oracle WebLogic Server, remove all the certificates that have SHA 256 RSA

encryption in the keystore (cacerts). For example, if you are using IBM JRE version 1.6 SR7, remove these three certificates: `secomscrootca2`, `keynectisrootca`, and `globalsignr3ca`.

Enabling SSL between Enterprise Manager and the directory service

Use the Enterprise Manager interface to enable SSL between Enterprise Manager and the directory service.

To enable SSL between Enterprise Manager and the directory service:

1. Start Enterprise Manager and log in as a GCD administrator.
2. In the tree view, right-click the root node and choose **Properties**.
3. In the Enterprise Manager Properties dialog box, click the **Directory Config.** tab, select a directory service, and click **Modify**.
4. In the **General** tab of the Modify Directory Configuration dialog box, set the **Is SSL Enabled** parameter to True and modify the port number appropriately.
5. Click **OK** in each open dialog box.

Enabling SSL between IBM Administration Console for Content Platform Engine and the directory service

You need to enable SSL between IBM Administration Console for Content Platform Engine and the directory service.

To enable SSL between IBM Administration Console for Content Platform Engine and the directory service:

1. Start IBM Administration Console for Content Platform Engine if you did not already do so:
 - a. On any computer, open a browser and navigate to `http://CPE_Server:port/acce`. *CPE_Server* is the name of the system where Content Platform Engine is deployed. *port* is the WSI port that used by the application server where Content Platform Engine is deployed.
 - b. Log on as the `gcd_admin` user.
2. Enable SSL between IBM Administration Console for Content Platform Engine and the directory service:
 - a. Select the domain node in the navigation pane.
 - b. Select **Properties** in the details pane, open the drop-down list for Directory Configurations, and select your directory server type.
 - c. Scroll to the **Is SSL Enabled** field and set its value to True.
 - d. Click **Close**.

Setting up Application Engine SSL security

You can configure an Application Engine to direct sign-ins through a Secure Socket Layer (SSL) https connection. This configuration takes place after you have installed and configured Application Engine.

Application Engine supports the following methods of configuring an SSL environment:

- Full SSL support - A single Application Engine server, where all of the software is running under SSL.

- One server SSL redirect - One Application Engine server set up to redirect logon attempts on the non-SSL port to the SSL port.
- Two server SSL redirect - Two Application Engine servers, where one is SSL-enabled, and the other redirects users to the SSL-enabled Application Engine server to log on.

“Setting up full SSL support on a single Application Engine”

To set up full SSL support, enable SSL on the preferred application server.

“Setting up SSL redirect on a single Application Engine server”

To set up SSL redirect, enable SSL on the preferred application server, set your bootstrap preferences, update the base URL, and sign out.

“Setting up SSL redirect on two Application Engine servers” on page 119

You can set up two-server SSL redirect for Application Engine. In this configuration, one Application Engine server is SSL-enabled, and the other Application Engine redirects users to the SSL-enabled Application Engine server to log on.

“Using Java Applets in an SSL Environment” on page 120

If you are using a Java applet in an SSL environment, you might experience an `SSLHandshakeException` because the appropriate certificate does not exist on your computer. Follow the instructions in the IBM FileNet P8 help topic

Working with documents and other content > Working with documents with Workplace > Tools > Publishing Designer > About Publishing Designer > Use Java applets to resolve this issue.

Setting up full SSL support on a single Application Engine

To set up full SSL support, enable SSL on the preferred application server.

To set up full SSL support on a single Application Engine:

1. Enable SSL on the application server that runs Application Engine (see your SSL documentation).
2. Test the SSL connection by signing into Workplace using the following URL:

`https://Application_Engine_server_name:SSL_port/Workplace`

The entire sign-in process will be handled by the SSL-enabled host.

Related concepts:



SSL port numbers

For more information about SSL port numbers, see *Plan and Prepare Your Environment for IBM FileNet P8*.

Setting up SSL redirect on a single Application Engine server

To set up SSL redirect, enable SSL on the preferred application server, set your bootstrap preferences, update the base URL, and sign out.

To set up SSL redirect on a single Application Engine server:

1. Enable SSL on the application server that runs Application Engine (see your SSL documentation).
2. Sign in to Workplace:
 - a. On any computer, open a browser and type the following URL address:
`http://Application_Engine_server_name:port#/Workplace`
 - b. Sign in as a user with Application Engine Administrator access role privileges. For more information, see the IBM FileNet P8 help topic **Working with documents and other content > Working with documents with Workplace XT > Site preferences > Access roles preferences**.

3. Set bootstrap preferences:
 - a. Navigate to **Admin Site Preferences > Bootstrap**.
 - b. Set the Security info Site Preference SSL Host:Port to identify the alias host name and port number.
Use the IP address of the Application Engine server for the SSL Host entry.
 - c. Click **Apply** to save your bootstrap settings.
4. Update the base URL:
 - a. Navigate to **Admin > Site Preferences > Refresh**.
 - b. Enter the Workplace Base URL value in the provided field. The URL must contain a valid host name, and not contain "localhost" or an IP number. For example, `http://myserver:7001/Workplace`
For more information, see the IBM FileNet P8 help topic **Working with documents and other content > Working with documents with Workplace XT > Site preferences > Refresh preferences**.
 - c. Click **Refresh** to update the base URL.
 - d. Click **Exit** to close Site Preferences.
5. Sign out of Workplace, and close your browser.
6. Test the SSL connection by signing in to Workplace using the following URL:
`http://Application_Engine_server_name:non-SSL port/Workplace`
You will be redirected to the SSL-enabled port for sign in, then back to the non-SSL enabled port after sign-in is complete. Before sign-in, you should receive a warning that you are accessing pages over a secure connection (unless you turned this dialog box off), and then Workplace will open.

Setting up SSL redirect on two Application Engine servers

You can set up two-server SSL redirect for Application Engine. In this configuration, one Application Engine server is SSL-enabled, and the other Application Engine redirects users to the SSL-enabled Application Engine server to log on.

1. Install Application Engine on both computers so that both Application Engine installations use the same `bootstrap.properties` file and site preferences file (the setup program will prompt you for a shared location).
During setup of the first Application Engine, create a share on the folder where the `bootstrap.properties` file is installed (the `\WEB-INF` folder). Then during setup of the second Application Engine, specify the shared location from the first installation. The `bootstrap.properties` file must already exist when specifying a shared location.

Important: The system clocks on the two Application Engine servers must be synchronized to within the Token time-out interval. For more information, see the IBM FileNet P8 help topic **Working with documents and other content > Working with documents with Workplace XT > Site preferences > Bootstrap site preferences > User tokens**.

2. Copy the `UTCryptokeyFile.properties` file.
For SSL redirect to work, each Application Engine must use the same User Token cryptographic key file.
After installing the second Application Engine, copy the `UTCryptokeyFile.properties` file from the first Application Engine server to the same location on the second Application Engine server.
Copy the file over a secure link.

3. Enable SSL on the application server that you are using for the SSL-enabled Application Engine (see your SSL documentation).
4. Sign in to Workplace on the non-SSL enabled Application Engine.
 - a. On any computer, open a browser and type:
`http://ApplicationEngineServerName:port#/Workplace`
 - b. Sign in as a user with Application Engine Administrator access role privileges. For more information, see the IBM FileNet P8 help topic **Working with documents and other content > Working with documents with Workplace XT > Site preferences > Access roles preferences**.
5. Set bootstrap preferences:
 - a. Navigate to **Admin > Site Preferences > Bootstrap**.
 - b. Set the Security info Site Preference SSL Host:Port to identify the alias host name and port number.
 - c. Click **Apply** to save your bootstrap settings.
6. Update the base URL:
 - a. Navigate to **Admin > Site Preferences > Refresh**.
 - b. Enter the Workplace Base URL value in the provided field. The URL must contain a valid host name, and not contain localhost or an IP number. For example, `http://myserver:7001/Workplace`
 For more information, see the IBM FileNet P8 help topic **Working with documents and other content > Working with documents with Workplace XT > Site preferences > Refresh preferences**.
 - c. Click **Refresh** to update the base URL.
 - d. Click **Exit** to close Site Preferences.
7. Sign out of Workplace, and close your browser.
8. Test the SSL connection by signing into Workplace using the following URL:
`http://Application_Engine_server_name:non-SSL port#/Workplace`
 You will be redirected to the SSL-enabled server for sign in, then back to the non-SSL enabled server after sign-in is complete. Before sign-in, you should receive a warning that you are accessing pages over a secure connection (unless you turned this dialog box off), and then Workplace will open.

Using Java Applets in an SSL Environment

If you are using a Java applet in an SSL environment, you might experience an `SSLHandshakeException` because the appropriate certificate does not exist on your computer. Follow the instructions in the IBM FileNet P8 help topic **Working with documents and other content > Working with documents with Workplace > Tools > Publishing Designer > About Publishing Designer > Use Java applets** to resolve this issue.

Performing additional configuration tasks

After you have completed the installation tasks, your core FileNet P8 system is operational. You can do the recommended additional configuration tasks to prepare the system for general use.


Except where noted, the topics in the following list are located in the FileNet P8 Information Center.

- Configure Content Federation Services for Image Services Guidelines. See the *IBM FileNet Content Federation Services for Image Services Planning and Configuration Guide*.

- Configure Application Engine to set the file types you want to open in a browser window rather than opening the Image Viewer. See **Administering FileNet P8 > Administering Application Engine > Application Engine Administration > Manage configuration files > Content redirection properties**.
- Set site preferences for the Workplace application. See **Working with documents and other content > Working with documents with Workplace > Tools > Publishing Designer > Security > Specify publication document security**.
- Design searches and/or search templates for Workplace users. See **Working with documents > Working with documents with Workplace > Tools > Search Designer**.
- Design publishing templates for Workplace users. See **Working with documents > Working with documents with Workplace > Tools > Publishing Designer**.
- Configure security for publishing. See **Working with documents > Working with documents with Workplace > Tools > Publishing Designer > Security > Specify publication document security > .**
- Configure automatic workflow launch. See **Administering FileNet P8 > Administering Content Platform Engine > Changing objects > Subscribing to events**.
- Create and configure the object stores that will contain business objects, folders, documents, workflow definitions, searches, and other objects. See **Installing additional FileNet P8 products > IBM FileNet Content Federation Services for Image Services configuration > Configuring IBM FileNet Content Federation Services for Image Services > Configuring the IBM FileNet Content Engine server > Creating an object store**.
- Define document classes and folders and set security for each class. See **Administering FileNet P8 > Administering Content Platform Engine > Adding documents and objects > Classifying documents > Classes > Concepts: Classes**.
- Review and, if necessary, edit the security of the network shared folders containing any file stores created for the object store. See **Administering FileNet P8 > Administering Content Platform Engine > Defining the repository infrastructure > Storing content > Storage area types > File storage areas**.
- Configure email notification. See **Administering FileNet P8 > Administering Content Platform Engine > Defining the workflow system > Configuring the workflow system > Enabling email notification**.
- Set workflow system runtime options. See **Integrating workflow into document management > Process Configuration Console > Managing the workflow system > Viewing or modifying workflow system properties > Setting runtime options**.
- Create a content cache area. See **Administering FileNet P8 > Administering Content Platform Engine > Defining the repository infrastructure > Storing content > Optimizing storage area performance > Creating a content cache area**.
- Create additional authentication realms. See **Security > FileNet P8 security > How to... > Configure multiple realms**.
- Define additional isolated regions. See **Administering FileNet P8 > Administering Content Platform Engine > Defining the workflow system > Configuring the workflow system > Creating additional connection points and isolated regions**.
- For each isolated region:
 - Define workflows. See **Integrating workflow into document management > Process Designer**.

- Configure event logging options. See **Integrating workflow into document management > Process Configuration Console > Isolated regions > Viewing or modifying isolated region properties > Configure event logging options.**
- Configure step processors. See **Integrating workflow into document management > Process Configuration Console > Isolated regions > Viewing or modifying isolated region properties > Configuring custom step processors.**
- Define and configure work queues. See **Integrating workflow into document management > Process Configuration Console > Configuring workflow queues.**
- Define and configure component queues. See **Integrating workflow into document management > Process Configuration Console > Manage component queues.**
- Define and configure workflow rosters. See **Integrating workflow into document management > Process Configuration Console > Configuring workflow rosters.**

Related information:

 [Product documentation for IBM FileNet P8 Platform](#)
Download the IBM FileNet P8 Platform documentation.

Optional installation tasks

You can install the additional or optional FileNet P8 components in any order.

“Installing and configuring IBM FileNet P8 publishing components”

For publishing capabilities, install the IBM FileNet Rendition Engine.

“Installing FileNet Deployment Manager”

You use FileNet Deployment Manager to deploy test systems into full production. You can install FileNet Deployment Manager interactively or silently.

“Installing Application Integration” on page 125

You can install Application Integration if you want to integrate IBM FileNet Workplace with your Microsoft Office applications and Outlook. You must complete the installation procedure on each machine that will use Workplace Application Integration.

“Deploying multiple Application Engine instances” on page 127

You can deploy multiple instances of Workplace on a single application server. Each deployment of Workplace must use the same Content Engine, Process Engine, and connection point.

“Enabling Application Engine to use ISRA” on page 130

Image Services Resource Adaptor (ISRA) is a Java EE connector to the IBM FileNet Image Services libraries. Using ISRA, Workplace users can view FileNet Image Services documents and their associated annotations in the FileNet Image Viewer and, if they have the appropriate permissions, update the annotations.

“Installing and configuring IBM System Dashboard for Enterprise Content Management” on page 134

Content Platform Engine and Application Engine install, by default, the necessary software required for IBM System Dashboard for Enterprise Content Management. To use the IBM System Dashboard for Enterprise Content Management software, you need to enable associated components and install IBM System Dashboard for Enterprise Content Management to perform related configuration procedures.

“Installing the COM compatibility layer (CCL)” on page 134

The option to install the COM compatibility layer is available as part of the FileNet P8 Content Platform Engine installation program.

Installing and configuring IBM FileNet P8 publishing components

For publishing capabilities, install the IBM FileNet Rendition Engine.

Install the IBM FileNet Rendition Engine to establish publishing capabilities. For instructions, see **Installing additional IBM FileNet P8 products > IBM FileNet Rendition Engine installation and upgrade**.

Installing FileNet Deployment Manager

You use FileNet Deployment Manager to deploy test systems into full production. You can install FileNet Deployment Manager interactively or silently.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

To install FileNet Deployment Manager:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Content Platform Engine values, filter by **CPE Installer** in the **Installation or Configuration Program** column.

2. Access the Content Platform Engine installation software.
3. Start the Tools installation. FileNet Deployment Manager is installed with the Content Platform Engine tools.

Option	Description
Interactive installation	<ol style="list-style-type: none"> 1. Run one of the following Content Platform Engine installation programs, depending on the operating system where you are installing FileNet Deployment Manager: <ul style="list-style-type: none"> • 5.2.0-P8CE-LINUX.BIN • 5.2.0-P8CE-WIN.EXE 2. To install FileNet Deployment Manager, choose only the Tools option in the installation program. 3. Complete the program installation wizard by using the values from your worksheet.
Silent installation	<ol style="list-style-type: none"> 1. Open the CE_silent_install.txt file in the software package for editing. 2. Set the parameter values in the CE_silent_install.txt file for your site. Be sure to set the CHOSEN_INSTALL_FEATURE_LIST parameter value to Tools 3. Set the LAUNCH_CM value to 0. 4. Save your edits. 5. Run one of the following Content Platform Engine installation programs, depending on the operating system where you are installing FileNet Deployment Manager: <ul style="list-style-type: none"> • 5.2.0-P8CE-LINUX.BIN -i silent -f CE_silent_install.txt • 5.2.0-P8CE-WIN.EXE -i silent -f CE_silent_install.txt

4. To start FileNet Deployment Manager:
 - (Windows only) Choose **Start > All Programs > IBM FileNet P8 Platform > FileNet Deployment Manager**.
 - (Linux only) Run this program (shown at the default installation location):
/opt/IBM/FileNet/ContentEngine/tools/deploy/DeploymentManager

Installing Application Integration

You can install Application Integration if you want to integrate IBM FileNet Workplace with your Microsoft Office applications and Outlook. You must complete the installation procedure on each machine that will use Workplace Application Integration.

“Installing Application Integration interactively”

You can access the Application Integration installation program from within the Workplace application. Complete the wizard screens to provide the appropriate values for your Application Integration installation.

“Installing Application Integration silently” on page 126

To install the Application Integration software silently, save the ApplicationIntegration.exe file locally and then run it at the command line using the /s switch.

“Verifying your Workplace Application Integration installation” on page 127

After you install Application Integration, you can verify your installation by trying the functions from within an integrated Microsoft application.

Installing Application Integration interactively

You can access the Application Integration installation program from within the Workplace application. Complete the wizard screens to provide the appropriate values for your Application Integration installation.

To install the Application Integration software interactively:

1. Log onto the client machine with an account that has Administrator privileges.
2. Sign in to Workplace.
3. Click **Author**, and then click **General Tools**.
4. Scroll down and click **Download Application Integration for Microsoft Office**, and then do one of the following:
 - Click **Open** to run the program from its current location.
 - Click **Save**. In the Save As dialog box, find a location on your machine in which to download and save the ApplicationIntegration.exe file locally, and then click **Save**. After the file is saved to your hard drive, double-click the file to run the installer.

The Welcome Wizard dialog box for Application Integration appears. Another Welcome dialog box appears.

5. Click **Next**.
6. Read the license agreement, and then select **I accept the terms to the license agreement**, and then click **Next**. If you do not accept the license agreement, you cannot continue with the install.
7. Do the following:
 - Select the applications you want to integrate, and then click **Next**.

Remember: The Application Integration Toolkit Components option is required to use Application Integration.

- Under **Install to**, the default installation path is displayed. Click **Change** to specify a different location on the Change Current® Destination Folder dialog box, and then click **OK**. Click **Next**.

You might see two default installation paths - one for Microsoft Office and Outlook, and another for the Toolkit Components. The Toolkit Components

path only appears when the system on which you are installing Application Integration has the Toolkit Components currently installed. You cannot modify the Toolkit Components installation path.

8. Enter the server name, port number and application name that defines the Workplace address. The *server name* is the name of the web server running Workplace, *port number* is the web server assigned port, *application* is the directory where you installed the Workplace application files.

Check **Server uses secure connection (SSL)** if you are running full SSL to encrypt all communication with Workplace.

You can also leave these fields blank and enter the information when you log on to Workplace Application Integration.

9. Click **Next**.
10. Click **Install**.
11. After the install is complete, click **Finish** to complete the setup process.

Installing Application Integration silently

To install the Application Integration software silently, save the ApplicationIntegration.exe file locally and then run it at the command line using the /s switch.

1. Log in to the client machine using an account that has Administrator privileges.
2. Sign in to Workplace.
3. Click **Author** , and then click **General Tools**.
4. Scroll down and click **Download Application Integration for Microsoft Office**, and then click **Save**. In the Save As dialog box, find a location on your machine in which to download and save the ApplicationIntegration.exe file locally, and then click **Save**.
5. Open a DOS command window and change the current directory to the one where ApplicationIntegration.exe resides.
6. Type the following at the command line:

```
ApplicationIntegration.exe /s/v"/qn <additional
msi arguments included in string>
LICENSE_ACCEPTED=true"
```

Use the /s switch to launch the execution silently and include the /qn switch in the msi string to make msi run silently.

See the following optional command line values you can also use. Append the values within the string containing the msi arguments. For example:

```
ApplicationIntegration.exe /s/v"/qn /L*v
C:\temp\AppIntSetup.txt LICENSE_ACCEPTED=true"
```

Table 29. Command line values and installations

Command Line Values	Installs
ADDLOCAL=ALL	All Features
ADDLOCAL=ALL REMOVE=OutlookIntegrationFeature	Office Only
ADDLOCAL=ALL REMOVE=OfficeIntegrationFeature	Outlook Only
ADDLOCAL=ALL REMOVE=OutlookIntegrationFeature,OfficeIntegrationFeature	Core Only

Table 30. Command line values and settings

Command Line Values	Settings
HOST=<host name>	Enter the name of the web server running Workplace.
PORT=<port number>	Enter the web server's assigned port number.
APPLICATION=<application name>	Enter the directory in which you installed the Workplace application files.
SERVER_CONNECTION=1	Set Application Integration to use an https connection
SERVER_CONNECTION=0	Set Application Integration to use http connection. This is the default if this parameter is not passed.
SINGLE_SIGNON=0	Set Application Integration to not use single sign-on (SSO).
SINGLE_SIGNON=1	Set Application Integration to use single sign-on (SSO).
/L*v C:\temp\AppIntSetup.txt	Verbose installation log and specify log location.

Verifying your Workplace Application Integration installation

After you install Application Integration, you can verify your installation by trying the functions from within an integrated Microsoft application.

1. Start Microsoft Word.
2. From the **File** menu, click **FileNet P8**, click **Open Document**, and then click **Select Item**. The Logon dialog box opens.
3. Log on with any valid domain account. The available object stores in your environment are displayed.

If you did not enter the Workplace Address information during the installation, you can enter the server name, port number, and application name that define the Workplace address. The server name is the name of the web server running Workplace, the port number is the assigned port of the web server, and the application is the directory where you installed the IBM FileNet P8 Workplace application files.

Check Server uses secure connection (SSL) if you use a full SSL to encrypt all communication with Workplace. Do not select this option if you use a SSL redirect during logon.

4. Close all dialog boxes and close Microsoft Word.

Deploying multiple Application Engine instances

You can deploy multiple instances of Workplace on a single application server. Each deployment of Workplace must use the same Content Engine, Process Engine, and connection point.

Each deployment of Workplace might use different Site Preference settings and might provide access to different object stores.

- The following procedure assumes that you have already installed Application Engine and performed the configuration tasks according to your application server type.
- When deploying multiple instances of Workplace, make copies of all the Workplace configuration and working files. Each instance of Workplace will use separate configuration, deploy, download, upload, and Workplace files. Leave the default installed files unmodified.
- For more information on how to deploy and manage multiple identical applications, see your application server documentation.

To deploy a second instance of the Workplace application:

“Deploying a second instance of Workplace”

Each deployment of Workplace might use different Site Preference settings and might provide access to different object stores.

“Deploying each additional Workplace instance as an EAR file” on page 129

You can choose to deploy your additional application instance as an EAR file.

You must perform the additional configuration for each custom Workplace instance you plan to deploy.

Deploying a second instance of Workplace

Each deployment of Workplace might use different Site Preference settings and might provide access to different object stores.

To deploy a second instance of the Workplace application:

1. Make a copy of the `/FileNet/Config/AE` directory, including all of its contents, for each instance you plan to deploy. For example, if you are deploying two instances, you would create:
`install_path/FileNet/Config/AE1`
`install_path/FileNet/Config/AE2`
2. Make copies of the upload and download directories in the `install_path/FileNet/AE` directory. For example, you would create:
`install_path/FileNet/AE/Download1`
`install_path/FileNet/AE/Upload1`
`install_path/FileNet/AE/Download2`
`install_path/FileNet/AE/Upload2`
3. Make a copy of the deploy directory and all of its contents for each Workplace instance. For example, you would create:
`install_path/FileNet/AE/deploy1`
`install_path/FileNet/AE/deploy2`
4. Make a copy the Workplace directory and all of its contents for each Workplace instance. For example, you would create:
`install_path/FileNet/AE/Workplace1`
`install_path/FileNet/AE/Workplace2`
5. Navigate to each custom copied Workplace `web.xml` instance and update the path for the configuration directory, upload directory, and download directory locations.

For example, in the `install_path/FileNet/AE/Workplace1/WEB-INF/web.xml`, you would make the following changes:

```
<context-param>
  <param-name>configurationDirectory</param-name>
  <param-value>opt/FileNet/Config/AE1</param-value>
```

```

</context-param>

<context-param>
<param-name>uploadDir</param-name>
<param-value>/opt/FileNet/AE/Upload1</param-value>
</context-param>
<context-param>
<param-name>downloadDir</param-name>
<param-value>/opt/FileNet/AE/Download1</param-value>
</context-param>

```

Deploying each additional Workplace instance as an EAR file

You can choose to deploy your additional application instance as an EAR file. You must perform the additional configuration for each custom Workplace instance you plan to deploy.

1. Modify the application.xml file located in the copied deploy directories, as follows:

- a. Open each instance of the application.xml file, for example, *install_path/FileNet/AE/deploy1/META-INF/application.xml*.
- b. Change the <display-name> and the <context-root> elements to your custom name, for example, Workplace1.

```

<display-name>Workplace1</display-name>
<description>FileNet Application Engine</description>

<module>
<web>
<web-uri>app_engine.war</web-uri>
<context-root>Workplace1</context-root>
</web>
</module>

```

2. In the create_app_engine_war file, set the install home and deploy directory to match your custom names.

For example, you would make the following changes:

```

install_home="/opt/FileNet/AE/Workplace1"
"${install_home}/../_AEjvm/bin/jar" -cf "${install_home}/../
deploy1/app_engine.war"*

```

3. In the create_app_engine_ear file, set the install home, deploy directory, and EAR file to match your custom names.

For example, you would make the following changes:

```

install_home="/opt/FileNet/AE/Workplace1"
cd "${install_home}/../deploy1"
"${install_home}/../_AEjvm/bin/jar" -cvf "${install_home}/../
deploy1/app_engine1.ear" META-INF *.war

```

4. Delete the existing app_engine.war and app_engine.ear files.
5. Create your custom WAR and EAR files by running the create_app_engine_war and then the create_app_engine_ear files.
6. Deploy the EAR file for each custom Workplace instance according to the procedures for your application server type.
7. Install any service packs, fix packs, or interim fixes required. To determine whether such additional software updates are needed, access the IBM FileNet P8 Platform support site.

Enabling Application Engine to use ISRA

Image Services Resource Adaptor (ISRA) is a Java EE connector to the IBM FileNet Image Services libraries. Using ISRA, Workplace users can view FileNet Image Services documents and their associated annotations in the FileNet Image Viewer and, if they have the appropriate permissions, update the annotations.

To enable Workplace users to view documents by using ISRA:

- Install Application Engine.
- Install FileNet Image Services Resource Adaptor.

For information on installing, configuring and deploying FileNet ISRA, See the Image Services Resource Adapter documentation in the FileNet ISRA installation package.

Tip: Use the Sample Application shipped with FileNet ISRA to confirm that the ISRA installation was successful.

Important: In an ISRA upgrade situation, take care to use the same library name (JNDI connection factory name) that has been previously set in the ISRA installation. Changing this variable can cause conflicts when accessing documents.

- Install the Application Engine ISRA Servlet and take the following into account:
 - Install and deploy ISRA before installing and deploying the ISRA Servlet.
 - Deploy the ISRA Servlet on the same application server as FileNet ISRA.
 - It is not necessary to install the ISRA Servlet on the Application Engine server. See “ISRA SSL support” on page 131 for details that might affect your collocation plans.
- Configure Workplace Site Preferences.

“ISRA SSL support” on page 131

The following table details supported SSL configurations for ISRA.

“Installing and deploying the Application Engine ISRA servlet” on page 131

To install and deploy the ISRA Servlet on the operating systems supported by Application Engine, run the associated ISRA setup program found in the Application Engine software package.

“Configuring Workplace site preferences for ISRA” on page 133

Before using the ISRA servlet, you must enable the FileNet Image Services external service and set the ISRA Interface Servlet URL in Workplace Site Preferences.

“Logging in to FileNet Image Services by using an LDAP account” on page 133

In order to log in to FileNet Image Services by using your LDAP account, you must configure ISRA for LDAP authentication.

“Accessing FileNet Image Services library documents” on page 134

For information about accessing FileNet Image Services library documents, see **Working with documents and other content > Working with documents with Workplace > Documents > Add a document.**

ISRA SSL support

The following table details supported SSL configurations for ISRA.

Table 31. SSL configuration and support

SSL Configuration	SSL Support
ISRA Servlet and Application Engine collocated. Application Engine configured for SSL logon redirect to a non-local host.	Supported
ISRA Servlet and Application Engine collocated. Application Engine configured for SSL logon redirect to a local host.	Supported
ISRA Servlet and Application Engine collocated. Application Engine and ISRA Servlet running under SSL.	Not Supported
ISRA Servlet remote from Application Engine. Application Engine configured for SSL logon redirect to a non-local host.	Supported
ISRA Servlet remote from Application Engine. Application Engine configured for SSL logon redirect to a local host.	Supported
ISRA Servlet remote from Application Engine. Application Engine running under SSL, ISRA Servlet not running under SSL.	Supported
ISRA Servlet remote from Application Engine. Application Engine and ISRA Servlet running under SSL.	Not Supported

Installing and deploying the Application Engine ISRA servlet

To install and deploy the ISRA Servlet on the operating systems supported by Application Engine, run the associated ISRA setup program found in the Application Engine software package.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

The Application Engine installation software contains the ISRA servlet installation programs for the supported Application Engine operating systems.

To install and deploy the Application Engine ISRA servlet:

1. Open your completed Installation and Upgrade Worksheet file.

Tip: In the worksheet file, verify that the **Data > Filter > AutoFilter** command is enabled. To view only Content Engine values, filter by **ISRA Installer** in the **Installation or Configuration Program** column.

2. Log on to the application server by using the following account, depending on your operating system:

Option	Description
AIX, HPUX, Linux, Linux for System z, Solaris	User account with write access to the /bin directory and read, write, and execute access to the directory where you plan to install ISRA Servlet.

3. Stop the application server instance if it is running.
4. Access the ISRA installation package, and start the following Application Engine ISRA Servlet setup program, depending on your operating system:

Option	Description
AIX, HPUX, Linux, Linux on System z, Solaris	AE-ISRA-Servlet-4.0.2.0-operating_system.bin

5. Complete the installation program screens by using the values from your worksheet.
6. Check the file `AE_ISRA_Servlet_install_log-4_0_2_0.txt`, located in the `AE_israservlet_install_path\FileNet` directory, to see if any errors occurred during the installation.

7. Install unlimited strength JAR files.

Perform this step only if the following are true:

- You selected the option to create Strong keys in the Application Engine User Token Security step of the Application Engine installation.
- Application Engine ISRA Servlet is deployed on a different application server than Application Engine.

Important: If these conditions are true, failure to perform this step causes an `EncryptionException` when you log on to the IS server.

8. (WebSphere Application Server and WebLogic Server only) Start the application server instance.
9. Deploy `AE_israservlet_install_path/FileNet/ApplicationEngineISRAServlet/ae_isra.war` in the same way you deployed the `app_engine.war` file for Workplace.
10. Verify the Application Engine ISRA Servlet is installed and deployed correctly, as follows. This step launches a diagnostic tool that does the verification.

- a. Open your web browser.
- b. Enter the URL for the Application Engine ISRA Servlet, for example:
`http://ApplicationEngineISRAServlet_servername:port/ApplicationEngineISRAServlet/ISRA`

`ApplicationEngineISRAServlet` is the default context root. If you specified a different name for the context root when deploying the Application Engine ISRA Servlet, change the URL to match your configuration.

If the ISRA Servlet is set up correctly, a congratulations message displays, for example:

Congratulations! ISRA Interface Servlet is configured at this URL.

```
WcmApiConfigFile = D:\ISRAInterface\jsp\WEB-INF\WcmApiConfig.properties
```

```
WcmApiConfig file exists
```

```
CryptoKeyFile/UserToken = C:\Program  
Files\FileNet\Authentication\UTCryptoKeyFile.properties
```

```
CryptoKeyFile/UserToken exists
```

```
FileNet ISRA classes are in the classpath
```

```
com.filenet.is.ra.cci.FN_IS_CciConnectionSpec
```


Related tasks:

Starting or stopping an application server instance

Configuring Workplace site preferences for ISRA

Before using the ISRA servlet, you must enable the FileNet Image Services external service and set the ISRA Interface Servlet URL in Workplace Site Preferences.

The Application Engine installation program installs the pre-configured Image Services external service, which includes the parameterized values necessary to access FileNet IS libraries from Workplace.

To configure Workplace Site Preferences for ISRA Servlet support:

1. Sign in to Workplace as a user having the Application Engine Administrators access role.
2. Launch Site Preferences as follows:
 - a. Select **Admin**.
 - b. Select **Site Preferences**.
3. Enable the pre-configured Image Services external service, as follows:
 - a. Select **External Services** from the left options list.
 - b. Select **Modify** for the Image Service, located under External Reference Services.

The External Reference Service Settings site preference page displays.
 - c. Under General Information, locate **Show on Select File page** and change the value to Show.
 - d. Accept the setting.
4. Set the ISRA Interface Servlet URL as follows:
 - a. Select **Bootstrap**.
 - b. Under Preferences Settings, set the value of ISRA Interface Servlet URL. For example:
`http://servername:port/ApplicationEngineISRAServlet/ISRA`
ApplicationEngineISRAServlet is the default context root. If you specified a different name for the context root when deploying the Application Engine ISRA Servlet, change the URL to match your configuration.
 - c. Accept the setting.
 - d. Exit Site Preferences.

Logging in to FileNet Image Services by using an LDAP account

In order to log in to FileNet Image Services by using your LDAP account, you must configure ISRA for LDAP authentication.

To log in to the FileNet Image Services library by using your LDAP account:

1. Configure ISRA for LDAP authentication.

For information on configuring LDAP authentication for ISRA, See the *ISRA Installation and Deployment Guide*. For information on configuring LDAP authentication for FileNet Image Services, See the *Image Services System Tools Reference Manual*.
2. Configure FileNet Image Services for LDAP authentication.

If the LDAP account with which you accessed Workplace is not valid for the FileNet Image Services library, or if LDAP authentication is not configured, you will be prompted to log in to the FileNet Image Services library.

Accessing FileNet Image Services library documents

For information about accessing FileNet Image Services library documents, see **Working with documents and other content > Working with documents with Workplace > Documents > Add a document**.

Installing and configuring IBM System Dashboard for Enterprise Content Management


Content Platform Engine and Application Engine install, by default, the necessary software required for IBM System Dashboard for Enterprise Content Management. To use the IBM System Dashboard for Enterprise Content Management software, you need to enable associated components and install IBM System Dashboard for Enterprise Content Management to perform related configuration procedures.

Installing IBM System Dashboard for Enterprise Content Management is not necessary if you currently have IBM Enterprise Content Management System Monitor installed.

See the IBM FileNet P8 help topic **Developing IBM FileNet P8 applications > FileNet System Manager Development** for instructions on how to enable the associated IBM System Dashboard for Enterprise Content Management components.

See the documentation provided with IBM System Dashboard for Enterprise Content Management for instructions on how to use the software.

Related information:

 Product documentation for installing IBM System Dashboard
Download the product documentation for IBM System Dashboard from the IBM FileNet P8 Platform documentation download page.

Installing the COM compatibility layer (CCL)

The option to install the COM compatibility layer is available as part of the FileNet P8 Content Platform Engine installation program.

To install the COM Compatibility Layer (CCL) from the Content Platform Engine installation program:

1. In the Choose Components dialog, select .NET Client, then click **Next**.
2. In the .NET API COM Compatibility Layer (CCL) Server URL dialog, enter a valid URL for the CCL (for example, `http://localhost:9080/wsi/FNCEWS40MTOM/`). Note that if you do not enter a valid URL, the CCL will not be installed.

If you do not install the CCL during the initial installation, you have the option of installation program later by running the Content Platform Engine installation program again. You can also install the CCL anytime by using the Configuration Manager tool.

Part 2. Removing software

Removing FileNet P8 software can involve deleting one or more core components, expansion products, and the FileNet P8 documentation.

“Removing the FileNet P8 documentation” on page 137

To remove the FileNet P8 documentation, you must remove the locally deployed Web application that contains the IBM FileNet P8 information center.

“Removing Content Platform Engine” on page 139

You can uninstall an entire Content Platform Engine installation or selected Content Platform Engine components.

“Removing IBM Content Search Services software” on page 141

“Removing Application Engine (WebSphere)” on page 143

Removal of the Application Engine for WebSphere on AIX, HP/UX, Linux, Linux for System z, Solaris, and Windows platforms requires that you log on to the application server and run the uninstall program.

“Removing Rendition Engine” on page 145

You can remove Rendition Engine software.

“Removing the Application Engine ISRA servlet” on page 147

Removal of the Application Engine ISRA Servlet for AIX, HP/UX, Linux, Linux for System z, or Windows environments requires that you logon to the application server, undeploy the servlet, and run the uninstall program.

Removing the FileNet P8 documentation

To remove the FileNet P8 documentation, you must remove the locally deployed Web application that contains the IBM FileNet P8 information center.

The procedure can be slightly different for each application server type and version. Use the documented procedures only for reference. Your specific installation directories and application names might vary.

“Removing the FileNet P8 documentation from a WebSphere Application Server”

To remove the FileNet P8 documentation from an application server, you must delete all the directories and files associated with the FileNet P8 information center. You must also delete the p8docs.war file that was installed by the FileNet P8 documentation installation program.

Removing the FileNet P8 documentation from a WebSphere Application Server

To remove the FileNet P8 documentation from an application server, you must delete all the directories and files associated with the FileNet P8 information center. You must also delete the p8docs.war file that was installed by the FileNet P8 documentation installation program.

To remove the FileNet P8 documentation:

1. Log on to the WebSphere Application Server computer that contains the FileNet P8 documentation.

Option	Description
AIX, HPUX, Linux, FileNet P8, Solaris	Log on as a user with delete access to the location where the FileNet P8 documentation files are installed.

2. Verify that the WebSphere Application Server is running.
3. From the WebSphere administrative console (for example, <http://localhost:9060/ibm/console>), choose **Uninstall** to remove the FileNet P8 documentation website, p8docs.
4. Delete the entire FileNet P8 documentation directory structure p8docs.war, from the installation location.
5. Delete any temp directories or log files for the FileNet P8 documentation.
Attention: Be careful not to accidentally remove any other FileNet P8 application files that are installed on the application server, for example, Workplace application files.
6. Run the following program file to remove the p8docs.war file that was installed by the FileNet P8 documentation installation program.

Option	Description
AIX, HPUX, Linux, FileNet P8, Solaris	From <i>p8docs.war_installation_path/</i> uninstall run <i>./uninstaller.bin</i> .

Removing Content Platform Engine

You can uninstall an entire Content Platform Engine installation or selected Content Platform Engine components.

Uninstalling Content Platform Engine does not undeploy it. You must use the application server console or commands to remove the Content Platform Engine EAR file from the application server.

Use one of the following procedures to uninstall part or all of Content Platform Engine.

“Removing an entire Content Platform Engine installation interactively (AIX, HPUX, Linux, Linux for System z, Solaris)”

To remove an entire Content Platform Engine installation, navigate to the *install_path/FileNet/ContentEngine/_ceuninst* directory and issue the following command: `ce_uninstaller`.

“Removing Content Platform Engine silently”

In silent mode, the uninstaller removes all Content Platform Engine components.

“Removing data associated with Content Platform Engine”

After uninstalling Content Platform Engine, you can remove its associated data.

Removing an entire Content Platform Engine installation interactively (AIX, HPUX, Linux, Linux for System z, Solaris)

To remove an entire Content Platform Engine installation, navigate to the *install_path/FileNet/ContentEngine/_ceuninst* directory and issue the following command: `ce_uninstaller`.

1. Navigate to the directory *install_path/FileNet/ContentEngine/_ceuninst*, created by the Content Platform Engine installer.
2. To uninstall Content Platform Engine interactively, run the following command: `ce_uninstaller`

Removing Content Platform Engine silently

In silent mode, the uninstaller removes all Content Platform Engine components.

To uninstall Content Platform Engine silently, run one of the following commands:

Option	Description
AIX, HPUX, Linux, Linux for System z, Solaris	<code>ce_uninstaller -i silent</code>

Removing data associated with Content Platform Engine

After uninstalling Content Platform Engine, you can remove its associated data.

1. Use the application server console or command lines to undeploy Content Platform Engine.

2. Use the application server console or command lines to remove any database JNDI data sources associated with Content Platform Engine object stores.
3. Use your database tools to drop any databases or table spaces for the object stores and the GCD.
4. Use your LDAP tools to delete users and groups you created in *Planning and Preparing for FileNet P8*.
5. Use your operating system commands to delete any directories, users, and groups that were used for installing and administering Content Platform Engine.
6. Use your operating system commands to delete any file-storage-area directories that contain content, such as documents.
7. Use your operating system commands to delete any index-area directories.

Removing IBM Content Search Services software

You can remove IBM Content Search Services software interactively or silently. Perform the appropriate tasks on your IBM Content Search Services server computer for the type of software removal you want to perform.

“Removing IBM Content Search Services interactively”

You must remove all of the existing IBM Content Search Services servers before you can completely remove IBM Content Search Services from your FileNet P8.

“Removing IBM Content Search Services silently”

You can remove IBM Content Search Services silently by setting the uninstallation value in an input response file and running the uninstallation program from a command line.

Removing IBM Content Search Services interactively

You must remove all of the existing IBM Content Search Services servers before you can completely remove IBM Content Search Services from your FileNet P8.

The IBM Content Search Services interactive uninstallation program removes the existing servers individually from your IBM FileNet P8 Platform. You can use the IBM Content Search Services silent uninstallation program to remove IBM Content Search Services in its entirety.

To remove IBM Content Search Services interactively:

1. Log in as *css_install_user*.
2. Access the IBM Content Search Services uninstallation package and run the *css_install_path/_cssuninst/css_uninstaller* (AIX, Linux, Solaris) or *css_uninstaller.exe* (Windows) file.
3. Select the IBM Content Search Services Server that you want to remove and click **OK** to uninstall the server.
4. (Optional) Repeat step 3 for each of the remaining servers you want to remove.
Attention: You must remove all of the servers before you can complete the IBM Content Search Services uninstallation.
5. Click **Uninstall** to remove the IBM Content Search Services product.
6. At the Uninstallation Complete window, click **OK**.
7. Remove the original server directories and the *css-servers.xml* file.
8. Review the *css_install_path/css_uninstall_5.2.0.log* file to verify that the uninstallation is complete.

Removing IBM Content Search Services silently

You can remove IBM Content Search Services silently by setting the uninstallation value in an input response file and running the uninstallation program from a command line.

The IBM Content Search Services interactive uninstallation program removes IBM Content Search Services servers from the system individually. Running the silent uninstallation program removes IBM Content Search Services in its entirety.

To remove IBM Content Search Services silently:

1. Log on to the host computer as *css_install_user*.
2. Open the *css_install_path/_cssuninst/installvariables.properties* file.
3. Go to the **SILENT_UNINSTALL_ALL** line and set the value to TRUE.
4. Save the edited response file to your temporary directory.
5. Go to the temporary directory on your local disk.
6. Run the IBM Content Search Services uninstallation program by running the appropriate command:

Table 32. Silent uninstallation commands

Platform	Command
Linux	<code>css_uninstaller -i silent -f installvariables.properties</code>

7. Remove the original server directories and the *css-servers.xml* file.
8. Review the *css_install_path/css_uninstall_5.0.0.log* file to verify that the uninstallation is complete.

Removing Application Engine (WebSphere)

Removal of the Application Engine for WebSphere on AIX, HPUX, Linux, Linux for System z, Solaris, and Windows platforms requires that you log on to the application server and run the uninstall program.

To remove the Application Engine software:

1. Log on to the application server.

Option	Description
AIX, HPUX, Linux, Linux for System z, Solaris	Log on as a user with read, write, and execute access to the directory where Application Engine is installed.

2. Log in to the WebSphere administrative console.
3. Uninstall the Workplace application.
 - a. Stop the Workplace process in the admin console.
 - b. Uninstall the Workplace application from Enterprise Applications.
4. Navigate to the `/_uninst` folder under the Application Engine installation location.
5. Run the uninstall program:

Option	Description
AIX, HPUX, Linux, Linux for System z, Solaris	uninstaller.bin

6. Delete the Workplace folder: `WAS_HOME/temp/node_name/application_server_name/Workplace`
7. Delete the `AE_install_path` directory.
8. (If Application Engine is the only IBM FileNet P8 application installed on the server) Search for the `vpd.properties` file. If it exists, delete it.

Important: In the following step, do not remove the system environment variable if any other IBM FileNet P8 application is installed on the server.

9. (AIX, HPUX, Linux, Linux for System z, Solaris) Remove the `P8TASKMAN_HOME` system environment variable.

If Application Engine is the only IBM FileNet P8 application running on the server you must remove the `P8TASKMAN_HOME` system environment variable to complete the uninstallation.

Removing Rendition Engine

You can remove Rendition Engine software.

For instructions on removing the Rendition Engine software, see **Installing additional IBM FileNet products > IBM FileNet Rendition Engine installation and upgrade > Removing Rendition Engine software**.

Removing the Application Engine ISRA servlet

Removal of the Application Engine ISRA Servlet for AIX, HPUNIX, Linux, Linux for System z, or Windows environments requires that you logon to the application server, undeploy the servlet, and run the uninstall program.

Since the installed names for the ISRA Servlet are configurable on the supported application servers, the following information might not be the same as your environment. Make the appropriate name changes as required for your environment.

To remove the Application Engine Servlet software:

1. Log on to the application server.

Option	Description
AIX, HPUX, Linux, Linux for System z, Solaris	Log on as a user with write access to the directory where ISRA Servlet is installed.

2. Undeploy the ApplicationEngineISRAServlet application. This step is similar to that required to undeploy the Workplace application.

Option	Description
IBM WebSphere Application Server	<ol style="list-style-type: none">1. Stop the ApplicationEngineISRAServlet process in the Admin console.2. Uninstall the ApplicationEngineISRAServlet application from Enterprise Applications.

3. Navigate to the /_uninstISRA directory under the ISRA Servlet installation location.

4. Run the uninstall program:

Option	Description
AIX, HPUX, Linux, Linux for System z, Solaris	uninstall.bin

5. Navigate to the /FileNet directory. If there is no other FileNet software installed under this directory, delete the /FileNet directory. If there is some other FileNet software installed under this directory, delete only the /ApplicationEngineISRAServlet subdirectory.
6. (WebSphere Application Server only) Delete the following temporary working folders for the Application Engine ISRA Servlet: *WAS_Home*\WebSphere\AppServer\profiles\default\installedApps\servername\ApplicationEngineISRAServlet.ear\

Part 3. Appendixes

Appendix A. Configuration Manager reference

Configuration Manager is a tool for configuring and deploying new or upgraded instances of the Content Platform Engine application on an application server.

You use Configuration Manager to define the following information for the Content Platform Engine instance:

- Application server properties
- Java Database Connectivity (JDBC) data source properties for the global configuration database (GCD)
- Java Database Connectivity (JDBC) data source properties for each object store database
- Directory service (LDAP) provider properties
- Content Platform Engine application login modules
- Content Platform Engine bootstrap and text extraction properties

“Overview of Configuration Manager” on page 152

You can use Configuration Manager to generate one or more unique Content Platform Engine configuration profiles. A profile is a collection of information required to configure and deploy new or upgraded Content Platform Engine instances.

“Handling passwords in Configuration Manager” on page 155

To provide the highest possible security, the default settings of Configuration Manager do not save passwords from the GUI application. The password save setting is a preference setting in the Configuration Manager graphical interface. While the default setting provides greater password security, it does require you to reenter all necessary passwords each time you start the GUI. When you close a profile in Configuration Manager, the passwords are removed from memory. When you open Configuration Manager or the profile again to run a saved task, you must reenter passwords to run the tasks.

“Accessing the Configuration Manager log files” on page 156

Configuration Manager generates task execution messages, log files for each task, and a log file for diagnosing Configuration Manager errors.

“Correcting a dotnetclient configuration profile error” on page 156

If you specified an incorrect value in the dotnetclient configuration profile .NET API COM Compatibility Layer (CCL) server URL during the installation of Content Platform Engine, you need to edit the `configmgr.properties` file to correct the error.

“Adding an SSL signer to the Configuration Manager keystore (WebSphere)” on page 157

If you are using SSL for communication between Configuration Manager and WebSphere Application Server you might receive an SSL signer error when you test the connection to the application server or when you run the Deploy Application task. To resolve the issue, make sure that you have an entry for the SSL signer in the truststore that Configuration Manager uses.

“Correcting an SSL Signer Exchange Prompt error (WebSphere)” on page 158

If you are using SSL for communication between Content Platform Engine and WebSphere Application Server, you might receive the SSL signer error SSL SIGNER EXCHANGE PROMPT when you run the task for configuring the JDBC data sources for the global configuration database (GCD) or for an object store.

“Configuration Manager user interface reference” on page 159

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content Platform Engine configuration profile. You can also make a copy of an existing profile, run configuration tasks, view the session logs, and check the status of a particular task.

“Configuration Manager command-line reference” on page 176

Configuration Manager can be run from a command line. This section covers the syntax for the command-line version of Configuration Manager.

Overview of Configuration Manager

You can use Configuration Manager to generate one or more unique Content Platform Engine configuration profiles. A profile is a collection of information required to configure and deploy new or upgraded Content Platform Engine instances.

“Configuration profile concepts”

The information for a profile is collected in XML files in the form of properties and values that describe the associated configuration and deployment tasks.

You must provide values for the profile properties that are specific to each configuration at your site, such as the application server name.

“Using the graphical and command-line user interfaces” on page 154

Both the graphical user interface (GUI) and the command-line interface (CLI) create the configuration XML files with the property values specific to your site, run tasks to apply your settings, display task status results, and deploy the Content Platform Engine application.

“Gathering Configuration Manager values by using the Installation and Upgrade Worksheet” on page 154

You can use the Installation and Upgrade Worksheet to record the values that you must enter in Configuration Manager.

Configuration profile concepts

The information for a profile is collected in XML files in the form of properties and values that describe the associated configuration and deployment tasks. You must provide values for the profile properties that are specific to each configuration at your site, such as the application server name.

The XML files are stored in a directory that is unique to a given profile. Because the profile name is used for both the directory name and the configuration file name, you must provide a profile name that is a valid directory name for your operating system. By default, the profiles are stored in the `ce_install_path/tools/configure/profiles` directory, where `ce_install_path` is the location where Content Platform Engine is installed.

If needed, you can create multiple profiles, each of which supports a unique Content Platform Engine instance. These instances can be located on the same server or on different servers, depending on your deployment preferences, the managed or non-managed nature of your application servers, and your clustering or high-availability requirements.

Use Configuration Manager to perform the following tasks that are associated with a Content Platform Engine configuration profile:

- **Set the application server properties.** Content Platform Engine will be deployed as an application on the application server. You must specify the application server type, the software version number, the server name, the administrative

user name and password, and other settings. The application server type determines some of the properties and their default values. All profiles include the application server properties. By default, the application server properties are stored in the *ce_install_path/tools/configure/profiles/myprofile/applicationserver.xml* file, where *myprofile* is the name of your profile.

You provide the application server properties when you create a profile by using the Create New Installation Profile wizard, and you can edit the application server properties at any time as needed. See “Creating a profile for a new installation” on page 167 or “Editing the application server properties” on page 169 for detailed procedures.

- **Configure the Java Database Connectivity (JDBC) data sources.** The JDBC data source information is used by Content Platform Engine to connect to global configuration database (GCD) and object store databases. The application server uses the JDBC data source information to connect Content Platform Engine to the database. You must specify the JDBC provider type, the database name, the database user name and password, and other settings. The JDBC provider type determines some of the properties and their default values. By default, the JDBC properties are stored in the *ce_install_path/tools/configure/profiles/myprofile/configurejdbcgcd.xml* file or the *ce_install_path/tools/configure/profiles/myprofile/configurejdbcos.xml* file, where *myprofile* is the name of your profile.

See “Editing the Configure JDBC Data Sources tasks” on page 169 for the procedure to set the JDBC data source properties after you have created a profile.

- **Configure the application login modules.** The login modules provide authentication information for the Content Platform Engine application. Run this task to create the login modules on the application server.

See “Editing the Configure LDAP task” on page 170 for the procedure to create the login modules after you have created a profile.

- **Configure the directory service (LDAP) provider.** Content Platform Engine connects to the directory service provider to authenticate users. Because the application server uses the directory service information to connect the Content Platform Engine to the directory service provider, you cannot skip this task even if you have already configured your application server prior to installing Content Platform Engine. You need to specify the directory service provider type, the user and group naming conventions for your provider, the directory service user name for the Content Platform Engine to use for authentication, and other settings. The LDAP provider type that you select determines some of the properties and their default values. By default, the LDAP properties are stored in the *ce_install_path/tools/configure/profiles/myprofile/configureldap.xml* file, where *myprofile* is the name of your profile.

See “Editing the Configure LDAP task” on page 170 for the procedure to set the LDAP properties after you have created a profile.

- **Configure the Content Platform Engine bootstrap and text extraction settings.** The bootstrap information is needed for creating the global configuration database and for starting Content Platform Engine. By default, the bootstrap properties are stored in the *ce_install_path/tools/configure/profiles/myprofile/configurebootstrap.xml* file, where *myprofile* is the name of your profile. The text extraction settings are for formatting text files so that they can be indexed.

See “Editing the Configure Bootstrap and Text Extraction task” on page 171 for the procedure to set the bootstrap properties after you have created a profile.

- **Deploy the Content Platform Engine application.** This action deploys the Content Platform Engine EAR file with the JDBC, LDAP, and bootstrap settings on the application server. Any time that you update the properties for an existing deployed Content Platform Engine instance or update the Process Engine Client files on the Content Platform Engine, you must redeploy for the changes to take effect. By default, the deployment properties are stored in the `ce_install_path/tools/configure/profiles/myprofile/deployapplication.xml` file, where *myprofile* is the name of your profile.

Tip: After you deploy the Content Platform Engine application, you use Enterprise Manager to customize Content Platform Engine for your site's requirements.

See “Editing the Deploy Application task” on page 171 for the procedure to edit the deployment properties after you have created a profile.

- Check the status of a particular configuration task. Status messages are displayed when you run a task. You can also explicitly display the task status any time after you run the task. See “Checking the task status” on page 175.
- **Configure a profile for upgrading an existing Content Platform Engine.** An upgrade profile includes the Configure Login Modules task, the Configure Bootstrap and Text Extraction task and the Deploy Application task. For JBoss Application Server, the profile also includes the Configure LDAP task. By default, the bootstrap and text extraction properties are stored in the `ce_install_path/tools/configure/profiles/myprofile/upgradebootstrap.xml` file, and the deployment properties are stored in the `ce_install_path/tools/configure/profiles/myprofile/deployapplication.xml` file, where *myprofile* is the name of your profile.

See “Creating a profile for a new installation” on page 167 for a detailed procedure.

Using the graphical and command-line user interfaces

Both the graphical user interface (GUI) and the command-line interface (CLI) create the configuration XML files with the property values specific to your site, run tasks to apply your settings, display task status results, and deploy the Content Platform Engine application.

Configuration Manager has a GUI and a CLI. The GUI version of the tool displays the properties and default values that you must set. When you save your changes in the GUI tool, the configuration XML files are updated for you. If you use the CLI version of the tool, you must first generate the configuration XML files with the tool, and then manually edit the default values in the files using a text editor. After you edit the files, you use Configuration Manager to run the tasks to apply the saved settings. After you have set the required values, you use either version of Configuration Manager to deploy the Content Platform Engine application.

The configuration XML files that you create with either version of the Configuration Manager tool can be used with the other version. For example, you can create the files with the CLI version, and then use the GUI version to open the profile, edit the values, and run the configuration tasks.

Gathering Configuration Manager values by using the Installation and Upgrade Worksheet

You can use the Installation and Upgrade Worksheet to record the values that you must enter in Configuration Manager.

Be sure that you have available the Installation and Upgrade Worksheet that was completed during your planning activities.

To see only the properties that you must specify for Configuration Manager:

1. Open your completed Installation and Upgrade Worksheet file.
2. Verify that the **Data > Filter > AutoFilter** command is enabled.
3. Filter by one of the following Configuration Manager options in the **Installation or Configuration Program** column:
 - **CM: config_mgr_user**
 - **CM: Create New Installation Profile**
 - **CM: Configure GCD JDBC Data Sources**
 - **CM: Configure Object Store JDBC Data Sources (object store 1)**
 - **CM: Configure LDAP**
 - **CM: Configure Bootstrap Properties and Text Extraction**
 - **CM: Deploy Application**
 - **CM: Upgrade bootstrap**
 - **CM: Upgrade Configuration Profile**

Handling passwords in Configuration Manager

To provide the highest possible security, the default settings of Configuration Manager do not save passwords from the GUI application. The password save setting is a preference setting in the Configuration Manager graphical interface. While the default setting provides greater password security, it does require you to reenter all necessary passwords each time you start the GUI. When you close a profile in Configuration Manager, the passwords are removed from memory. When you open Configuration Manager or the profile again to run a saved task, you must reenter passwords to run the tasks.

The following passwords are used to run the tasks:

- The application server administrator password. Select **File > Edit Application Server Properties** to enter the password.
- The database administrator password. Edit the **Configure GCD JDBC Data Sources** task or the **Configure Object Store JDBC Data Sources** task.
- The directory service bind user password. Edit the **Configure LDAP** task.
- The bootstrap user password. Edit the **Configure Bootstrap and Text Extraction** task.

The Configuration Manager command line passes the passwords from an XML configuration file to the required application when you run a task. You can use the **storepasswords** command to add encrypted passwords to the XML files, or you can enter plain text passwords when you edit the files. However, saving the passwords to the XML files might not be FIPS 140-2 compliant.

If you later use the Configuration Manager GUI to open a profile with an XML configuration file that you manually edited, the GUI version reads the passwords in the XML file, and will overwrite the existing passwords when you save the file. If the GUI is not configured to save passwords (default setting), the passwords in the XML file will be overwritten with a blank entry. If the GUI is configured to save passwords, the original values or any changed values are encrypted and saved to the XML file.

Accessing the Configuration Manager log files

Configuration Manager generates task execution messages, log files for each task, and a log file for diagnosing Configuration Manager errors.

- When you run a task in the Configuration Manager graphical user interface, the task execution messages are displayed in the console pane. When you run the task in the command-line interface, the messages are written in the command window.
- In the **Content Platform Engine Task View** of the graphical user interface, you can view additional status in the console by right-clicking the task and then selecting **Check Task Status**. See “Checking the task status” on page 175 for details. In the command-line interface, use the **checkstatus** command within **configmgr_cl** to determine the status of each task. For example, to determine the deployment status, run this command:

```
configmgr_cl checkstatus -profile profile_name -task deployapplication
```
- The log file for each Configuration Manager task that you execute is located in the temporary directory that you specified for the task. For example, the **configureldap** task puts two files into the *ce_install_path/tools/configure/tmp* directory:

Log file	Description
configureldap.tcl	The running version of the script
configureldap.log	The details log file

- The .log file contains additional information for diagnosing Configuration Manager errors. The path to the file depends on the platform:

Platform	Path
AIX, HPUX, Linux, Linux on System z, Solaris	<i>user_home_directory</i> /configmgr_workspace/.metadata/.log

For example, on Windows the path might be C:\Documents and Settings\Administrator\configmgr_workspace\.metadata\.log.

Correcting a dotnetclient configuration profile error

If you specified an incorrect value in the dotnetclient configuration profile .NET API COM Compatibility Layer (CCL) server URL during the installation of Content Platform Engine, you need to edit the configmgr.properties file to correct the error.

To correct a dotnetclient configuration profile error:

1. Open the configmgr.properties file for editing. This file is located at *ce_install_path/tools/configure/configuration/*
2. Find the line in the file that starts with CCL_URL:

```
CCL_URL=http://localhost:port_number/wsi/FNCEWS40MTOM/
```
3. Use the graphical user interface or the command-line interface of Configuration Manager to reexecute the dotnetclient profile. If you use the command-line interface, run this command to reexecute the profile:

```
configmgr_cl execute -task configureDotNetAPI -profile dotnetclient
```

Adding an SSL signer to the Configuration Manager keystore (WebSphere)

If you are using SSL for communication between Configuration Manager and WebSphere Application Server you might receive an SSL signer error when you test the connection to the application server or when you run the Deploy Application task. To resolve the issue, make sure that you have an entry for the SSL signer in the truststore that Configuration Manager uses.

1. Identify the serial number for the SSL certificate on the web application server.
 - a. From the server where Configuration Manager is installed, browse to the WebSphere administrative console address.
 - b. In the Security Alert dialog box, click **View Certificate**.
 - c. Click the **Details** tab.
 - d. Record the value for **Serial number** for the certificate.
 - e. Click **OK** to dismiss the Certificate dialog box.
 - f. Click **Yes** in the Security Alert dialog box to proceed.
2. Identify the truststore location and filename.
 - a. Log in to the WebSphere administrative console.
 - b. Select **Security > SSL certificate and key management**.
 - c. Select **SSL configurations**.
 - d. Click the default SSL setting, **NodeDefaultSSLSettings**.
 - e. Under the **Related items** link, click **Key stores and certificates**.
 - f. Record the filename, such as `trust.p12`, in the **Path** column of the resource to be updated:

Table 33. Resources to be updated

Application server type	Name of resource to be updated
IBM WebSphere Application Server	NodeDefaultTrustStore
Clusters built on IBM WebSphere Application Server Network Deployment	CellDefaultSSLSettings

3. Start IBM Key Management by entering one of the following commands at a command prompt:

Option	Description
AIX, HPUX, Linux, Linux on System z, Solaris	<code>WAS-Home/AppServer/bin/ikeman.sh</code>

4. Select **Keybase File > Open**.
 - a. For the **Key database type**, select **PKCS12**.
 - b. Click **Browse** to locate the filename you recorded in step 2. For example, the File Name field contains the filename, such as `trust.p12`. The **Location** field contains the absolute path to the truststore, such as `C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\etc\` for Windows.
 - c. Click **OK**.
 - d. Enter the password and click **OK**. The default password is `WebAS`.
5. Locate the signer certificate with the serial number that matches the serial number that you recorded in step 1.
 - a. Double-click a certificate name other than **default_signer** to view the serial number for the certificate.

- b. Click **OK** to close the dialog box.
 - c. Repeat until you have located the correct signer certificate.
6. Extract the certificate.
 - a. Select the signer certificate with the correct serial number, and click **Extract**.
 - b. Provide a name and location, and then click **OK**.
7. Add the certificate that you extracted to the trust file for Content Platform Engine.
 - a. Open the DummyClientTrustFile.jks key database file located in the WebSphere profile for Content Platform Engine, such as C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\etc\ for Windows.
 - b. Add the certificate that you extracted in step 6.
8. Close IBM Key Management.

Correcting an SSL Signer Exchange Prompt error (WebSphere)

If you are using SSL for communication between Content Platform Engine and WebSphere Application Server, you might receive the SSL signer error SSL SIGNER EXCHANGE PROMPT when you run the task for configuring the JDBC data sources for the global configuration database (GCD) or for an object store.

Use this procedure if you receive the following error when you run a task for configuring the JDBC data sources, such as **Configure GCD JDBC Data Sources**:

```
Error while executing Configure GCD JDBC Data Sources
Execution failed with the following message: The data source configuration failed.
*** SSL SIGNER EXCHANGE PROMPT ***
SSL signer from target host null is not found in trust store
```

1. From a command prompt, navigate to the *WAS_HOME/AppServer/profiles/app_server_name/bin* directory.
2. Run the following command:


```
wsadmin.bat -conntype SOAP -port portnumber -username username
-passwd userpassword
```

Where:

portnumber
is the same value that you entered for the **Application server SOAP** field in the configure JDBC task properties. The WebSphere default is 8880.

username
is the same value that you entered for the **Application server administrator user name** field in the configure JDBC task properties.

userpassword
is the same value that you entered for the **Application server administrator password** field in the configure JDBC task properties.
3. At the prompt to add the signer to the trust store, enter Yes.
4. Close the command prompt.
5. Use Configuration Manager to run the configure JDBC task again, from the graphical user interface or from the command line.

Configuration Manager user interface reference

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content Platform Engine configuration profile. You can also make a copy of an existing profile, run configuration tasks, view the session logs, and check the status of a particular task.

Restriction: If you need an accessible version of Configuration Manager, use the command line interface instead of the GUI. See “Configuration Manager command-line reference” on page 176.

“Starting Configuration Manager”

You can start the graphical interface version of Configuration Manager to configure a Content Platform Engine application instance on a web application server.

“Configuration Manager window” on page 160

The default Configuration Manager window consists of the Content Platform Engine Task View pane on the left side, the Task Editor pane on the upper right side, and the Console pane on the lower right side. You can drag, resize, and rearrange the panes to change the location if needed.

“Configuration Manager menus and commands” on page 162

You can access the Configuration Manager commands through the menu or by right-clicking an item. The following tables describe the available commands.

“Working with Configuration Manager” on page 165

You can use the Configuration Manager commands, icons, and panes to work with your profiles and configuration tasks.

“configmgr.ini parameters” on page 176

When you install Configuration Manager, the path to the directory that contains the Java binary to be used to launch the graphical user interface is added to the `ce_install_path/tools/configure/configmgr.ini` file.

Starting Configuration Manager

You can start the graphical interface version of Configuration Manager to configure a Content Platform Engine application instance on a web application server.

See the appendix “Configuration Manager user interface reference” for complete information about using the graphical user interface. If you need an accessible version of Configuration Manager, use the command-line interface instead of the graphical user interface.

To start Configuration Manager:

1. Start Configuration Manager by running one of the following commands, depending on the operating system that runs on the machine where you installed Content Platform Engine, and log on as the `config_mgr_user`:

Option	Description
AIX, Solaris, HP-UX, HP-UXi, Linux, Linux for System z	Run this command: <code>ce_install_path/tools/configure/configmgr</code>

The first time that you start Configuration Manager, the Welcome is displayed.

2. Select one of the links in the Welcome to learn more or to start working in a wizard, or close the Welcome by clicking the **X** in the tab at the upper left. You can reopen the Welcome later, as needed, from the **Help** menu.

Configuration Manager window

The default Configuration Manager window consists of the Content Platform Engine Task View pane on the left side, the Task Editor pane on the upper right side, and the Console pane on the lower right side. You can drag, resize, and rearrange the panes to change the location if needed.

Pane	Description
Content Platform Engine Task View	Displays a profile and the tasks for that profile. Only one profile can be open at a time.
Task Editor	Displays the properties and values for a selected task. The Task Editor pane is empty until a specific task is selected from the Content Platform Engine Task View pane. Each open task is displayed in a separate tab in the Task Editor pane. More than one task tab can be displayed at a time.
Console	Displays task execution messages, results from the Check Status command, or the session log.

To move from one open task tab in the Task Editor pane to another open task tab, press **Ctrl-F6**.

To move from one pane to the next, press **Ctrl-F7**.

To restore a closed pane, select **Window > Show View**.

“Main toolbar”

The Configuration Manager main toolbar is located just below the menu bar. The main toolbar contains multiple icons for working with your profiles.

“Profile toolbar” on page 161

The Configuration Manager profile toolbar is located at the upper right of the Content Platform Engine Task View pane. The profile toolbar contains multiple icons for working with a selected profile.

“Console toolbar” on page 161

The Console toolbar is located at the upper right of the Console pane. The Console toolbar contains the multiple icons for working with the Console pane.




Main toolbar

The Configuration Manager main toolbar is located just below the menu bar. The main toolbar contains multiple icons for working with your profiles.

Table 34. Main toolbar icons and commands



Icon	Command name and description
	New Installation Profile Click this icon to create a profile for a new installation. The current configuration profile will be closed, and the New Configuration Profile Wizard starts. If the existing open profile has been changed, you will be prompted to save your changes.

Table 34. Main toolbar icons and commands (continued)

Icon	Command name and description
	<p>New Upgrade Profile</p> <p>Click this icon to create a profile for upgrading an existing Content Engine server. The current configuration profile will be closed, and if there have been changes, you will be prompted to save your changes. The New Configuration Profile Wizard starts.</p>
Open Profile	<p>Open Profile</p> <p>Click this icon to open an existing profile. The current configuration profile will be closed, and if there have been changes, you will be prompted to save your changes.</p>
	<p>Save</p> <p>Click this icon to save the current configuration profile settings.</p>
	<p>View Configuration Manager Log File</p> <p>Click this icon to view the Configuration Manager session log. The session log is cleared when you open Configuration Manager or when you close a profile.</p>

Profile toolbar

The Configuration Manager profile toolbar is located at the upper right of the Content Platform Engine Task View pane. The profile toolbar contains multiple icons for working with a selected profile.

Icon	Command name and Description
	<p>Edit Application Server Properties</p> <p>Click this icon to view or edit the application server properties for the current profile.</p>
	<p>Run All Tasks</p> <p>Click this icon to run all the enabled tasks for the current profile.</p>

Console toolbar

The Console toolbar is located at the upper right of the Console pane. The Console toolbar contains the multiple icons for working with the Console pane.

Table 35. Console toolbar icons and commands






Icon	Command name and description
	<p>Clear Console</p> <p>Click this icon to clear the display for the currently active tab in the Console pane. Clearing the display does not affect any log contents.</p>

Table 35. Console toolbar icons and commands (continued)

Icon	Command name and description
	<p>Scroll Lock</p> <p>Click this icon to enable or disable the scroll bars for the currently active tab in the Console pane. When the scroll bars are locked, information in the console might scroll out of view.</p>
	<p>Pin Console</p> <p>Click this icon to lock or unlock the current console location. When pinned (or locked), you cannot move the Console pane to a new location or resize the Console pane.</p>
	<p>Display Selected Console</p> <p>Click this icon to select the console tab to display. Select the desired tab from the list of recently viewed consoles.</p>
	<p>Open Console</p> <p>Click this icon to new tab with the current Console view. For example, you can open a second tab for execution messages for the Deploy Application task.</p>

Configuration Manager menus and commands

You can access the Configuration Manager commands through the menu or by right-clicking an item. The following tables describe the available commands.

Main menu

The following table lists the menus and commands that are available in Configuration Manager.

Table 36. Main menu commands

Menu name	Command name	Description
File		Provides commands for creating, saving, or opening a configuration profile.
	New Installation Profile	Creates a profile for a new installation. See “Creating a profile for a new installation” on page 167 for detailed procedures to create a profile.
	Upgrade Profile	Creates a profile for upgrading Content Platform Engine. See “Creating a profile for an upgrade” on page 167 for detailed procedures to create a profile.
	Edit Application Server Properties	Opens the Edit Application Server Properties wizard for editing the application server values for the profile.
	Open Profile	Opens an existing profile for viewing or editing.
	Close Profile	Closes the current profile.
	Save	Saves your changes to the active task.
	Save All	Saves your changes to all open tasks.

Table 36. Main menu commands (continued)

Menu name	Command name	Description
	Save Copy of Profile As	Saves the current profile with a new name or path.
	Run All Tasks	Runs all of the tasks in the profile to apply your settings. If a particular task is disabled, that task is skipped when you select Run All Tasks.
	Exit	Closes Configuration Manager.
Window		Provides commands for viewing a log file, changing the view in a Configuration Manager pane, and setting preferences.
	View Log File in Console	Provides commands that give you access to logs and various views of information.
	Show View	Displays the session log in the Console pane. The session log lists results from tasks that you have run since you opened the current profile.
	Preferences	Provides choices for determining the behavior of Configuration Manager, such as the password save preference and the warning message preference.
Help		Displays help pages about Configuration Manager.
	Welcome	Provides a quick introduction to the use of Configuration Manager.
	Help Contents	Provides reference information for Configuration Manager.
	About Configuration Manager for Content Platform Engine	Displays the copyright and related information about Configuration Manager.

Pop-Up menus

The pop-up menus are displayed when you right-click an item in Configuration Manager. The following table shows all the possible commands. The commands that you actually see in your Add New Task pop-up menu depend on which tasks are in your profile.

Table 37. Profile Icon Pop-Up Menu Commands

Command	Description
Edit Application Server Properties	Opens the Edit Application Server Properties wizard for the profile.
Run All Tasks	Displays a submenu of the tasks associated with the profile. Click the task name that you want to run.
Close Profile	Closes the configuration profile.
Add New Task > Configure GCD JDBC Data Sources	Adds a Configure GCD JDBC Data Sources task to the profile. You cannot have more than one Configure GCD JDBC Data Sources task in a profile.
Add New Task > Configure Object Store JDBC Data Sources	Adds a New_Configure Object Store JDBC Data Sources task to the profile. You can have multiple Configure Object Store JDBC Data Sources tasks in a profile.

Table 37. Profile Icon Pop-Up Menu Commands (continued)

Command	Description
Add New Task > Configure Login Modules	Adds a Configure Login Modules task to the profile. You cannot have more than one Configure Login Modules task in a profile.
Add New Task > Configure LDAP	Adds a Configure LDAP task to the profile. You can have multiple Configure LDAP tasks in a profile.
Add New Task > Configure Bootstrap and Text Extraction	Adds a Configure Bootstrap and Text Extraction task to the profile. You can have multiple Configure Bootstrap and Text Extraction tasks in a profile.
Add New Task > Deploy Application	Adds a Deploy Application task to the profile. You cannot have more than one Deploy Application task in a profile.

Table 38. Task Icon Pop-Up Menu Commands

Command	Description
Edit Selected Task	Opens the task in the task pane for editing.
Run Task	Runs the selected task.
Check Task Status	Displays the current status of the task.
Enable Task	Toggles the state of the task between enabled and disabled. Any task that is disabled will not run with either the Run Task command or the Run All Tasks command. If the task is currently enabled, selecting the Disable Task command prevents the task from running, changes the font for the task icon to italic, and appends (disabled) to the icon label. If the task is currently disabled, selecting the Enable Task command allows the task to run, restores the original font, and removes (disabled) from the icon label.
Disable Task	
Rename Task	Opens an edit window in which you can change the name of the label associated with the task.
Copy Selected Task	Creates a copy of the selected task. This command is available only for the Configure Object Store JDBC Data Sources and the Configure LDAP tasks.
Add New Task > Configure GCD JDBC Data Sources	Adds a Configure GCD JDBC Data Sources task to the profile. You cannot have more than one Configure GCD JDBC Data Sources task in a profile.
Add New Task > Configure Object Store JDBC Data Sources	Adds a Configure Object Store JDBC Data Sources task to the profile. You can have multiple Configure Object Store JDBC Data Sources tasks in a profile.
Add New Task > Configure Login Modules	Adds a Configure Login Modules task to the profile. You cannot have more than one Configure Login Modules task in a profile.
Add New Task > Configure LDAP	Adds a Configure LDAP task to the profile. You can have multiple Configure LDAP tasks in a profile.
Add New Task > Configure Bootstrap and Text Extraction	Adds a Configure Bootstrap and Text Extraction task to the profile. You can have multiple Configure Bootstrap and Text Extraction tasks in a profile.
Add New Task > Deploy Application	Adds a Deploy Application task to the profile. You cannot have more than one Deploy Application task in a profile.
Reset Selected Task Status	Resets the status of the task to indicate that it has not yet been run.

Table 38. Task Icon Pop-Up Menu Commands (continued)

Command	Description
Delete Selected Task	Deletes the task from the profile. You cannot delete a task if it is open for editing in the task pane.
Move Selected Task Up	Moves the selected task up in the list of tasks.
Move Selected Task Down	Moves the selected task down in the list of tasks.

Working with Configuration Manager

You can use the Configuration Manager commands, icons, and panes to work with your profiles and configuration tasks.

“Configuring a Content Platform Engine instance” on page 166

You can use the Configuration Manager graphical user interface to configure a Content Platform Engine instance.

“Setting the password save preference” on page 166

By default, the Configuration Manager password save preference is set to not save passwords to a file. If your site security requirements permit you to save passwords to a file, you can change the password save preference setting.

“Creating a profile for a new installation” on page 167

You must create a new configuration profile for each Content Platform Engine application that you deploy.

“Creating a profile for an upgrade” on page 167

You use the upgrade configuration profile to update the existing Content Platform Engine bootstrap properties and deploy the updated EAR file. In order to create an upgrade profile, the Content Platform Engine installation program must have detected an existing Content Platform Engine installation.

“Opening and closing an existing profile or task” on page 168

You can save a profile, and open it later to edit the saved settings or to run tasks.

“Editing the application server properties” on page 169

You initially provide the application server properties when you create a new profile. You can open the application server properties for editing at any time, but you cannot change the application server type for an existing profile. The application server properties must be set before you run any tasks.

“Editing the properties for a specific task” on page 169

You must provide the required property values for each task in your profile before you run the task.

“Applying the property settings by running a specific task” on page 172

You must run a task to apply the values that you provided.

“Adding a task to a profile” on page 174

A profile can contain an unlimited number of tasks. You can configure more than one Configure Object Store JDBC Data Sources task, more than one Configure LDAP task, or more than one Configure Bootstrap and Text Extraction task. You can add a new task for a task type that you do not already have in the profile.

“Deleting a task from a profile” on page 174

You can delete any unneeded tasks from your profile.

“Running all tasks at the same time” on page 175

You can run all the tasks in a profile at the same time. Disabled tasks do not run.

“Running a single task” on page 175

You can run each configuration task individually. Disabled tasks will not run.

“Checking the task status” on page 175

Task execution messages are displayed in the console pane when you run a task, and you can view the status of a specific task at any time.

“Viewing the session log” on page 176

The session log contains information about the tasks that were run in the current session of Configuration Manager. As you run additional tasks for the same or a different profile, new messages are added to the log. When you exit Configuration Manager, the session log is cleared.

“Saving your changes to a task or profile” on page 176

You can save your profile and task settings at any time.

Configuring a Content Platform Engine instance

You can use the Configuration Manager graphical user interface to configure a Content Platform Engine instance.

To configure a Content Platform Engine instance:

1. Create a configuration profile. See “Creating a profile for a new installation” on page 167.
2. Edit the configuration tasks included in the profile. See one or more of the following topics:
 - “Editing the Configure JDBC Data Sources tasks” on page 169
 - “Editing the Configure LDAP task” on page 170
 - “Editing the Configure Login Modules task” on page 170
 - “Editing the Configure Bootstrap and Text Extraction task” on page 171
3. Apply the configuration settings by running the tasks. See “Running all tasks at the same time” on page 175.
4. Deploy the application by running the Deploy Application task. Because deployment can take a long time, it is a best practice to run the Deploy Application task after you have completed all other configuration tasks. See “Editing the Deploy Application task” on page 171.

Setting the password save preference

By default, the Configuration Manager password save preference is set to not save passwords to a file. If your site security requirements permit you to save passwords to a file, you can change the password save preference setting.

When you close the profile, the passwords are erased from memory. Each time that you start Configuration Manager or open a saved profile, the passwords are blank (unless you previously changed the preferences setting). Before you can run a task, you must specify the passwords required by the task and the application server properties; otherwise, the task will not run successfully. If your site security requirements permit you to save passwords to a file, you can change the password save preference setting.

To change the password save preference:

1. Click **Window > Preferences**.
2. Complete one of the following actions:

Option	Description
To save passwords to file	Select the Save all passwords to file when saving a task or profile check box.
To prevent writing passwords to file	Clear the Save all passwords to file when saving a task or profile check box.

3. Click **OK**.

Creating a profile for a new installation

You must create a new configuration profile for each Content Platform Engine application that you deploy.

To create a new configuration profile:

1. Start the Create New Installation Profile wizard by one of the following methods:
 - Click the **Create a profile for a new installation** icon in the toolbar.
 - Select **File > New Installation Profile**.
2. If a profile is already open, the Action Required message box opens. Respond to the messages as follows:
 - a. Click **Yes** to continue creating a new profile, or click **No** to cancel. If you selected **Yes** and your current profile has any unsaved changes, the Save Resource message box opens.
 - b. Click **Yes** to save your changes, or click **No** to continue without saving your changes.

The Create New Installation Profile wizard opens.
3. Complete the wizard screens. For details on the fields in the wizard screens, hover your mouse over the field name to view the field description.

The new profile is displayed as an icon in the left-hand pane with icons for the tasks that you selected. The default profile contains the following tasks:

- Configure GCD JDBC Data Sources
- Configure Object Store JDBC Data Sources
- Configure Login Modules
- Configure LDAP
- Configure Bootstrap and Text Extraction
- Deploy Application

Creating a profile for an upgrade

You use the upgrade configuration profile to update the existing Content Platform Engine bootstrap properties and deploy the updated EAR file. In order to create an upgrade profile, the Content Platform Engine installation program must have detected an existing Content Platform Engine installation.

To create a profile for an upgrade:

1. Start the Upgrade Configuration Profile wizard by selecting **File > Upgrade Profile**.
2. If a profile is already open, the Action Required message box opens. Respond to the messages as follows:
 - a. Click **Yes** to continue creating a new profile, or click **No** to cancel.

- b. If you selected **Yes** and your current profile has any unsaved changes, the Save Resource message box opens. Click **Yes** to save your changes, click **No** to continue without saving your changes, or click **Cancel**.
3. Complete the wizard screens. For details on the fields in the wizard screens, hover your mouse over the field name to view the property description.

The profile you created is displayed as an icon in the left pane with the name that was presented in the confirmation screen with icons for the following tasks:

- Configure LDAP
- Configure Login Modules
- Configure Bootstrap and Text Extraction
- Deploy Application

Opening and closing an existing profile or task

You can save a profile, and open it later to edit the saved settings or to run tasks.

To open or close an existing profile or task:

1. Open a profile by one of the following methods:
 - Click the **Open Profile** icon in the toolbar.
 - Select **File > Open Profile**.
 - a. If a profile is already open, the Action Required message box opens. Respond to the messages as follows:
 - 1) Click **Yes** to continue creating a new profile, or click **No** to cancel.
 - 2) If you selected **Yes** and your profile has any unsaved changes, the Save Resource message box opens. Click **Yes** to save your changes, click **No** to continue without saving your changes, or click **Cancel**.
 - b. Either type in the fully qualified path to the *myprofile.cfgp* profile file, or click **Browse** to locate the file.
 - c. Click **OK**.
2. Open a task:

More than one task tab can be open at a time in the Task Editor pane.

 - a. If the profile is collapsed in the Content Platform Engine Task View pane, click **+** next to the profile name to expand it.
 - b. Use one of the following methods to open the desired task:
 - Click the *task name* in the Content Platform Engine Task View pane, and then click **Edit Selected Task** in the Profile toolbar.
 - Double-click the *task name* in the Content Platform Engine Task View pane.
3. Switch between open tasks in the Task Editor pane by clicking the *tab name* in the Task Editor pane for the desired task.
4. Close a task:
 - a. If the task is not the actively selected task, click the *tab name* in the Task Editor pane for the desired task.
 - b. Click **Close** in the tab for the task. You will be prompted to save any changes to the task.
5. Close the profile by selecting **File > Close Profile**.

You will be prompted to save any changes when you close a profile. Passwords are removed from memory when you close a profile.

Editing the application server properties

You initially provide the application server properties when you create a new profile. You can open the application server properties for editing at any time, but you cannot change the application server type for an existing profile. The application server properties must be set before you run any tasks.

To edit the application server properties:

1. Start the Edit Application Server Properties wizard by using one of these methods:
 - Click **Edit Application Server Properties** in the profile toolbar.
 - Select **File > Edit Application Server Properties**.
2. Provide values for the application server properties. For details on the fields, hover your mouse over the field name to view the property description.
3. Optional: WebSphere Application Server and Oracle WebLogic Server only. In the Set Properties for Application Server window, click **Test Connection** to test the connection between Configuration Manager and the application server by using the information that you have provided. The test is optional, and you can proceed in the wizard even if the test fails, although most of the configuration tasks will fail to complete. If the test fails, make sure that the application server is running and that the application server property values that you entered match the values that are defined in your application server.
4. Click **Finish**.

Editing the properties for a specific task

You must provide the required property values for each task in your profile before you run the task.

“Editing the Configure JDBC Data Sources tasks”

The JDBC data source information is used by Content Platform Engine to connect to the global configuration database (GCD) and the object store databases. Configuration Manager provides two tasks for configuring the JDBC data sources: Configure GCD JDBC Data Sources and Configure Object Store JDBC Data Sources.

“Editing the Configure Login Modules task” on page 170

The login modules provide authentication information for the Content Platform Engine application.

“Editing the Configure LDAP task” on page 170

The LDAP information is used to connect Content Platform Engine to the directory service provider to authenticate users.

“Editing the Configure Bootstrap and Text Extraction task” on page 171

The bootstrap and text extraction information is needed for creating the global configuration database and for starting Content Platform Engine.

“Editing the Deploy Application task” on page 171

You can edit the deployment property values without applying the settings. When you apply the settings, the Content Platform Engine is deployed as an application on the application server. Because deploying an application can take time, we recommend that you do not deploy the application until after you have installed any dependent files, such as IBM Content Search Services, or customized applications for Content Platform Engine.

Editing the Configure JDBC Data Sources tasks:

The JDBC data source information is used by Content Platform Engine to connect to the global configuration database (GCD) and the object store databases.

Configuration Manager provides two tasks for configuring the JDBC data sources: Configure GCD JDBC Data Sources and Configure Object Store JDBC Data Sources.

The procedures for editing the Configure GCD JDBC Data Sources task and the Configure Object Store JDBC Data Sources task are the same. To complete the Content Platform Engine configuration, you must configure the GCD data sources and the data sources for each object store.

To edit the Configure JDBC Data Sources task:

1. Open either the GCD data source task or the object store data source task for editing:
 - Double-click **Configure GCD JDBC Data Sources**.
 - Double-click **Configure Object Store JDBC Data Sources**.
2. Provide the property values for your database. Place your mouse on a ? icon to view the property description.
3. Optional: WebSphere Application Server and Oracle WebLogic Server only. Click **Test Database Connection** to test the connection to the database by using the database user name, database server name, database name, port number, and password that you provided. The test does not create the data sources.
4. Select **File > Save** to save your changes. Saving your changes to disk does not apply the settings to the application server.

Editing the Configure Login Modules task:

The login modules provide authentication information for the Content Platform Engine application.

You do not need to provide any information to create the login modules. If needed, you can change the default values for the script file to run and for the temporary directory location.

To edit the Configure Login Modules task:

1. Make sure that the task is enabled. When the task is disabled, the task name includes the text **(Disabled)**. To enable the task, select **Configure Login Modules (Disabled)** in the profile pane, and then either right-click and choose **Enable Task** from the context menu, or click the **Enable Task** icon in the task toolbar. For details on the fields, hover your mouse over the ? icon to view the property description.
2. Create the login modules by right-clicking **Configure Login Modules** in the profile pane, and selecting **Run Task**. Running the configuration task can take a few minutes. The task execution status messages are displayed in the console pane below the bootstrap properties.

Tip: You can check the completion status of the task by right-clicking **Configure Login Modules** in the profile pane, and selecting **Check Task Status**.

3. Close the Configure Login Modules task pane.

Editing the Configure LDAP task:

The LDAP information is used to connect Content Platform Engine to the directory service provider to authenticate users.

To edit the Configure LDAP task:

1. Double-click **Configure LDAP** in the Content Platform Engine Task View pane to open the task for editing.
2. Provide the property values for your LDAP provider. For details on the fields, hover your mouse over the ? icon to view the property description.
3. Optional: WebSphere Application Server and Oracle WebLogic Server only. Click **Test LDAP Connection** to test the connection to the directory service provider by using the directory service bind user name, host name, port number, and password that you provided.
4. Select **File > Save** to save your changes.

Editing the Configure Bootstrap and Text Extraction task:

The bootstrap and text extraction information is needed for creating the global configuration database and for starting Content Platform Engine.

To edit the Configure Bootstrap and Text Extraction task:

1. Double-click **Configure Bootstrap and Text Extraction** in the Content Platform EngineTask View pane to open the task for editing.
2. Select a value for the **Bootstrap operation** field:

Option	Description
To provide bootstrap and text extraction information for a new installation profile	Select Configure New .
To upgrade an existing deployed EAR file	Select Upgrade .
To modify an existing deployed EAR file	Select Modify Existing .

3. Provide the bootstrap and text extraction property values. For details on the fields, hover your mouse over the ? icon to view the property description.
4. Optional: If you selected **Modify Existing** or **Upgrade**, click **View Bootstrapped EAR and Text Extraction Info** to display the modified bootstrap and text extraction information in the EAR file.
5. Select **File > Save** to save your changes.

Editing the Deploy Application task:

You can edit the deployment property values without applying the settings. When you apply the settings, the Content Platform Engine is deployed as an application on the application server. Because deploying an application can take time, we recommend that you do not deploy the application until after you have installed any dependent files, such as IBM Content Search Services, or customized applications for Content Platform Engine.

To edit the Deploy Application task:

1. Right-click the **Deploy Application** task in the profile pane (left pane), and select **Edit Selected Task**.
2. Provide the property values for your deployment. For details on the fields, hover your mouse over the ? icon to view the property description.
3. Select **File > Save**.

Related tasks:

“Configuring Content Platform Engine” on page 17

You can configure and deploy all of your Content Platform Engine instances with Configuration Manager. Configuration Manager prepares the Content Platform Engine application for deployment on the application server. A single Content Platform Engine application instance equates to one deployed application on your application server.

Applying the property settings by running a specific task

You must run a task to apply the values that you provided.

“Applying the JDBC data source settings”

Your JDBC data source settings are stored when you save the task, but the settings are not applied to the application server until you run the task.

“Applying the login module settings”

Your login module settings are stored when you save the task, but the settings are not applied to the application server until you run the task.

“Applying the LDAP settings” on page 173

Your LDAP settings are stored when you save the task, but the settings are not applied to the application server until you run the task.

“Applying the bootstrap and text extraction settings” on page 173

The bootstrap and text extraction information is needed for creating the global configuration database and for starting Content Platform Engine. Your bootstrap and text extraction settings are stored when you save the task, but the settings are not applied to the application server until you run the task.

“Deploying the application” on page 173

Your Deploy Application task settings are stored when you save the task, but the Content Platform Engine EAR file is not deployed to the application server until you run the task.

Applying the JDBC data source settings:

Your JDBC data source settings are stored when you save the task, but the settings are not applied to the application server until you run the task.

To apply the JDBC data source settings:

1. Select the configure data sources task that you want to run:
 - Right-click **Configure GCD JDBC Data Sources** in the Content Platform Engine Task View pane, and select **Run Task**.
 - Right-click **Configure Object Store JDBC Data Sources** in the Content Platform Engine Task View pane, and select **Run Task**.

Running the configuration task can take a few minutes.

2. Close the Configure JDBC Data Sources task pane.

The task execution status messages are displayed in the Console pane below the JDBC data source properties.

Applying the login module settings:

Your login module settings are stored when you save the task, but the settings are not applied to the application server until you run the task.

To apply the LDAP settings:

1. Right-click **Configure Login Modules** in the Content Platform Engine Task View pane, and then select **Run Task**. Running the configuration task can take a few minutes.
2. Close the Configure Login Modules task pane.

The task execution status messages are displayed in the Console pane below the Login Modules properties.

Applying the LDAP settings:

Your LDAP settings are stored when you save the task, but the settings are not applied to the application server until you run the task.

To apply the LDAP settings:

1. Right-click **Configure LDAP** in the Content Platform Engine Task View pane, and then select **Run Task**. Running the configuration task can take a few minutes.
2. Close the Configure LDAP task pane.

The task execution status messages are displayed in the Console pane below the LDAP properties.

Applying the bootstrap and text extraction settings:

The bootstrap and text extraction information is needed for creating the global configuration database and for starting Content Platform Engine. Your bootstrap and text extraction settings are stored when you save the task, but the settings are not applied to the application server until you run the task.

To apply the bootstrap and text extraction settings:

1. Right-click **Configure Bootstrap and Text Extraction Properties** in the Content Platform Engine Task View pane, and then select **Run Task**. Running the configuration task can take a few minutes.
2. Optional: If you selected **Configure New**, click **View Bootstrapped EAR and Text Extraction Info** to display the bootstrap and text extraction information in the EAR file.
3. Close the **Configure Bootstrap and Text Extraction** task pane.

The task execution status messages are displayed in the Console pane below the bootstrap properties.

Deploying the application:

Your Deploy Application task settings are stored when you save the task, but the Content Platform Engine EAR file is not deployed to the application server until you run the task.

To deploy the application:

1. Right-click the **Deploy Application** task in the left pane, and then select **Run Task**. Running the deployment task will take a few minutes.
2. Close the **Deploy Application** task pane.

The task execution status messages are displayed in the Console pane below the Deploy Application task properties.

Adding a task to a profile

A profile can contain an unlimited number of tasks. You can configure more than one Configure Object Store JDBC Data Sources task, more than one Configure LDAP task, or more than one Configure Bootstrap and Text Extraction task. You can add a new task for a task type that you do not already have in the profile.

The default configuration profile contains the following tasks:

- Configure GCD JDBC Data Sources
- Configure Object Store JDBC Data Sources
- Configure Login Modules
- Configure LDAP
- Configure Bootstrap and Text Extraction
- Deploy Application

You can add a new task whenever the following conditions apply:

- You do not already have an existing task of that type in the profile. You can have only one Configure GCD JDBC Data Sources task or one Deploy Application task.
- You have more than one object store in your site.
- You have multiple LDAP realms in your site.
- You must modify or upgrade you bootstrap properties.

To add a task to your profile:

1. If your configuration profile is not open in Configuration Manager, open the profile.
2. Right-click any *task name* in the profile pane, and select **Add New Task**.
3. In the pop-up menu, select the *task name* that you want to create. The new task is added to the profile. If a task of the same type exists, the new task name begins with **New_**.
4. Optional: Rename the task to provide a more useful name.
 - a. Right-click the new *task name*, and select **Rename Task**.
 - b. Enter a useful name for the task, such as Configure Object Store 2 JDBC Data Sources or Configure Bootstrap and Text Extraction for Upgrade.
 - c. Click **OK**.

Deleting a task from a profile

You can delete any unneeded tasks from your profile.

The default configuration profile contains the following tasks:

- Configure GCD JDBC Data Sources
- Configure Object Store JDBC Data Sources
- Configure Login Modules
- Configure LDAP
- Configure Bootstrap and Text Extraction
- Deploy Application

When you delete a task, all its property values are removed. If you later need the task, you must add a new task and reenter all your values.

To delete a task from a profile:

1. If your configuration profile is not open in Configuration Manager, open the profile.
2. Right-click the *task name* that you want to remove, and select **Delete Selected Task**.
3. In the confirmation message box, click **OK**.

Running all tasks at the same time

You can run all the tasks in a profile at the same time. Disabled tasks do not run.

To run all tasks in a profile:

1. If the profile is collapsed in the Content Platform Engine Task View pane, click + next to the profile name to expand it.
2. Use one of the following methods to run the Run All Tasks command:
 - Click **Run All Tasks** in the Content Platform Engine Task View pane toolbar.
 - Select **File > Run All**.

Important: Tasks do not complete if you did not enter passwords correctly during the current Configuration Manager session. See “Handling passwords in Configuration Manager” on page 155.

The Console pane displays the task execution messages.

Running a single task

You can run each configuration task individually. Disabled tasks will not run.

To run a selected task:

1. If the profile is collapsed in the Content Platform Engine Task View pane, click + next to the profile name to expand it.
2. Right-click the *task name* in the Content Platform Engine Task View pane, and select **Run Task** from the context menu.

Important: Tasks will not complete if you have not entered passwords correctly during the current Configuration Manager session. See “Handling passwords in Configuration Manager” on page 155.

The Console pane displays the task execution messages.

Checking the task status

Task execution messages are displayed in the console pane when you run a task, and you can view the status of a specific task at any time.

To check the task status:

1. If the profile is collapsed in the Content Platform Engine Task View pane, click + next to the profile name to expand it.
2. Right-click the *task name* in the Content Platform Engine Task View pane, and select **Check Task Status** from the context menu.

The console pane opens with the status listed for the selected task. The following table lists the status results and their descriptions.

Table 39. Task status in the console pane

Status Result	Description
COMPLETED	The task ran successfully.

Table 39. Task status in the console pane (continued)

Status Result	Description
INCOMPLETE	The task is incomplete.
NO STATUS AVAILABLE	The task has not been run.
FAILED	The task failed to complete. Additional information about the failure is displayed.

Viewing the session log

The session log contains information about the tasks that were run in the current session of Configuration Manager. As you run additional tasks for the same or a different profile, new messages are added to the log. When you exit Configuration Manager, the session log is cleared.

To view the session log:

1. Run at least one task.
2. Use one of the following methods to run the View Log command:
 - Click the **View the Configuration Manager Log File** icon in the Main toolbar.
 - Select **Window > View Log File in Console**.

The current session log is displayed in the Console pane. Subsequently running a task will replace the displayed session log with the current task status. To redisplay the session log, repeat this procedure as needed.

Saving your changes to a task or profile

You can save your profile and task settings at any time.

To save your changes to a task or profile:

Use one of these methods to save changes to the currently open task:

- Click **Save** in the toolbar.
- Select **File > Save**.

configmgr.ini parameters

When you install Configuration Manager, the path to the directory that contains the Java binary to be used to launch the graphical user interface is added to the `ce_install_path/tools/configure/configmgr.ini` file.

AIX, HPUNIX, Linux, Linux on System z, or Solaris example

```
-vm  
/opt/IBM/FileNet/ContentEngine/_cejvm/jre/bin
```

Configuration Manager command-line reference

Configuration Manager can be run from a command line. This section covers the syntax for the command-line version of Configuration Manager.

“Running Configuration Manager commands” on page 177

From the command line, you can generate the configuration XML files, run a configuration task to apply the settings in the configuration XML file, and check the status of a task. Use the following syntax to enter the Configuration Manager commands.

Running Configuration Manager commands

From the command line, you can generate the configuration XML files, run a configuration task to apply the settings in the configuration XML file, and check the status of a task. Use the following syntax to enter the Configuration Manager commands.

Use one of these commands to run the Configuration Manager command line:

Table 40. Configuration Manager commands

Operating System	File Name
AIX, HPUX, Linux, Linux on System z, Solaris	<code>ce_install_path/tools/configure/configmgr_cl</code>

“How to read the syntax diagrams”

Syntax diagrams describe how you must enter commands and what options are available.

“**checkstatus** command” on page 178

The **checkstatus** command checks the status of the specified configuration task. The command name is not case sensitive.

“**execute** command” on page 182

The **execute** command applies the settings from a configuration XML file for the specified configuration task. The command name is not case sensitive.

“**generateconfig** command” on page 185

The **generateconfig** command generates the configuration XML file for the specified configuration task. The command name is not case sensitive.

“**gui** command” on page 191

The **gui** command opens the Configuration Manager graphical user interface. The command is not case sensitive.

“**listtasks** command” on page 191

The **listtasks** command displays a list of the tasks and the task files in the configuration profile. The command name is not case sensitive.

“**movetask** command” on page 194

The **movetask** command moves a task to a different position in the list of tasks. The task position determines the order that the tasks are run when you run all the tasks at the same time. You use the **listtask** command to display the task order. The command names are not case sensitive.

“**removetask** command” on page 197

The **removetask** command removes the specified task from the configuration profile. When you remove the task, the configuration XML file is deleted from the profile directory. The command name is not case sensitive.

“**storepasswords** command” on page 200

The **storepasswords** command prompts for passwords that are blank in a profile and stores the encrypted passwords in the file. Storing encrypted passwords might not be FIPS 140-2 compliant. You can run the command for a single task or for all tasks in the profile. The command name is not case sensitive.

How to read the syntax diagrams

Syntax diagrams describe how you must enter commands and what options are available.

The syntax topics uses several conventions to indicate variable, parameters, required items, and optional items. Enter all commands on a single line, even if the command or syntax examples wrap to the next line.

```
command_name -option_1 variable_1 [-option_2 variable_2]
[-option_3 variable_3 | -option_4]
```

Where:

command_name

The **command_name** is required.

-option_1

The **-option_1** parameter is a required parameter.

variable_1

The *variable_1* value is a required variable for the **-option_1** parameter.

[-option_2 variable_2]

Square braces [] indicate optional items. The **-option_2** parameter with its value is optional.

-option_3 variable_3 | -option_4

A vertical bar indicates a choice of parameters. Use the **-option_3** parameter with its value, or use the **-option_4** parameter. In this example, both items are optional, and you can use only one or the other.

checkstatus command

The **checkstatus** command checks the status of the specified configuration task. The command name is not case sensitive.

checkstatus command syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line, without any line breaks.

```
configmgr_cl checkstatus [-task task_type | -taskfile task_file_name]
-profile myprofile [-help]
```

checkstatus command parameters

-task task_type

The **-task task_type** parameter specifies which task to use for the status check. You can omit the **-task task_type** parameter if you want to check all of the tasks or if you specify the **-taskfile task_file_name** parameter. The *task_type* value is not case sensitive. The following table lists the valid task names, the associated configuration XML file, and a description of the Content Platform Engine settings affected by the task.

Table 41. *task_type* values

Option	Configuration file	Description
omitted	configurebootstrap.xml configurejdbcgcd.xml configurejdbcos.xml configurejdbcos. <i>n</i> .xml configureldap.xml configureldap. <i>n</i> .xml configureloginmodules.xml deployapplication.xml Where <i>n</i> is an integer starting with 2	If you omit the <code>-task <i>task_type</i></code> parameter and the <code>-taskfile <i>task_file_name</i></code> parameter, then the status for all the configuration files in the profile is displayed.
configurebootstrap	configurebootstrap.xml	Checks status for applying the settings for the Content Platform Engine bootstrap and text extraction on the application server. The bootstrap information is needed for creating the global configuration database and for starting Content Platform Engine.
configurejdbcgcd	configurejdbcgcd.xml	Checks the status for configuring the JDBC connections to the global configuration database used by Content Platform Engine.

Table 41. *task_type* values (continued)

Option	Configuration file	Description
configurejdbcos	configurejdbcos.xml configurejdbcos. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	<p>Checks the status for configuring JDBC connections to a single object store database used by Content Platform Engine. You need to generate, edit, and apply the configurejdbcos task settings for each object store in your database.</p> <p>When you generate a second object store JDBC configuration file, it is named configurejdbcos.2.xml. The filename increments for each new file you generate. You cannot change the filename, but you can edit the value in the file for the name of the task.</p> <p>If your profile contains more than one configurejdbcos task, then you must specify the -taskfile <i>task_file_name</i> parameter to identify the task to check.</p>
configureLDAP	configureldap.xml configureldap. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	<p>Checks status for configuring the connection to the directory server for authenticating Content Platform Engine users.</p> <p>(WebSphere Application Server or Oracle WebLogic Server only.) If you generate a second LDAP configuration file, then it is named configureldap.2.xml. The filename increments for each new file you generate. You cannot change the filename, but you can edit the value in the file for the name of the task.</p> <p>If your profile contains more than one ConfigureLDAP task, then you must specify the -taskfile <i>task_file_name</i> parameter to identify the task to check.</p>

Table 41. *task_type* values (continued)

Option	Configuration file	Description
configureloginmodules	configureloginmodules.xml	(WebSphere Application Server or JBoss Application Server only.) Checks status for creating the login modules for the Content Platform Engine application.
deployapplication	deployapplication.xml	Checks status for deploying the Content Platform Engine application on the application server.

-taskfile *task_file_name*

The **-taskfile** *task_file_name* parameter specifies the configuration XML file to use.

If only one task file exists for the *task_type*, then the **-taskfile** *task_file_name* parameter is optional.

If more than one task file for the *task_type* exists, then you must include the **-taskfile** *task_file_name* parameter. You can omit the **-task** *task_type* parameter when you specify the **-taskfile** *task_file_name* parameter.

-profile *myprofile*

The **-profile** *myprofile* parameter specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as *ce_was_tiv_db2*. The profile must be located in the *ce_install_path*/tools/configure/profiles directory, where *ce_install_path* is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2" or /opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2.
- The absolute path to the profile input file, such as "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg" or /opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg".

-help

The **-help** parameter is optional and displays a brief message on the command syntax instead of running the command.

checkstatus command examples

The following examples include line breaks to format the command for reading. Enter the command and options on a single line, without any line breaks.

Check the status of a profile with only one file for the configurejdbcos task.

The following command checks the status of the configurejdbcos task in the *ce_install_path*/tools/configure/profiles/wstdb2jdbc directory:


```
configmgr_cl checkstatus -task configurejbcos -profile wstdb2jdbc
```

Check the status of a profile with several files for the configurejbcos task.

The following command checks the status of the configurejbcos.2.xml task file in the *ce_install_path/tools/configure/profiles/wstdb2jdbc* directory:

```
configmgr_cl checkstatus -taskfile configurejbcos.2.xml  
-profile wstdb2jdbc
```

Check the status for creating the login modules.

The following command checks the status of the configureloginmodules task in the *ce_install_path/tools/configure/profiles/wstdb2jdbc* directory:

```
configmgr_cl checkstatus -task configureloginmodules  
-profile wstdb2jdbc
```

Display the help for the checkstatus command.

The following command displays the help for the **checkstatus** command:

```
configmgr_cl checkstatus -help
```

execute command

The **execute** command applies the settings from a configuration XML file for the specified configuration task. The command name is not case sensitive.

execute command syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line, without any line breaks.

```
configmgr_cl execute [-task task_type | -taskfile task_file_name]  
-profile myprofile [-silent] [-force] [-help]
```

execute command parameters

-task *task_type*

The **-task *task_type*** parameter indicates which task to run. You can omit the **-task *task_type*** parameter if you want to run all of the tasks or if you specify the **-taskfile *task_file_name*** parameter. The *task_type* value is not case sensitive. The following table lists the valid task names, the associated configuration XML file, and a description of the Content Platform Engine settings affected by the task.

Table 42. *task_name* values

Option	Configuration file to execute	Description
omitted	configurebootstrap.xml configurejdbcgcd.xml configurejdbcos.xml configurejdbcos. <i>n</i> .xml configureldap.xml configureldap. <i>n</i> .xml configureloginmodules.xml deployapplication.xml where <i>n</i> is an integer starting with 2	If you omit the <code>-task task_type</code> parameter and the <code>-taskfile task_file_name</code> parameter, then all the configuration files in the path are run. Any configuration XML file that has the enabled attribute value in the <configuration> tag set to false is skipped.
configurebootstrap	configurebootstrap.xml	Applies the settings for the Content Platform Engine bootstrap text extraction on the application server. The bootstrap information is needed for creating the global configuration database and for starting Content Platform Engine.
configurejdbcgcd	configurejdbcgcd.xml	Applies the settings for configuring the JDBC connections to the global configuration database used by Content Platform Engine.
configurejdbcos	configurejdbcos.xml configurejdbcos. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Applies the settings for configuring JDBC connections to a single object store database used by Content Platform Engine. You need to generate, edit, and apply the configurejdbcos task settings for each object store in your database. When you generate a second object store JDBC configuration file, it is named configurejdbcos.2.xml. The filename increments for each new file you generate. You can edit the file name as needed. If your profile contains more than one configurejdbcos task, then you must specify the <code>-taskfile task_file_name</code> parameter to identify the task to run.

Table 42. *task_name* values (continued)

Option	Configuration file to execute	Description
configureldap	configureldap.xml configureldap. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Configures the connection to the directory server for authenticating Content Platform Engine users. WebSphere Application Server or Oracle WebLogic Server only.) If you generate a second LDAP configuration file, then it is named configureldap.2.xml. The filename increments for each new file you generate. You can rename the file as needed. If your profile contains more than one configureldap task, then you must specify the -taskfile <i>task_file_name</i> parameter to identify the task to run.
configureloginmodules	configureloginmodules.xml	(WebSphere Application Server or JBoss Application Server only.) Creates the login modules for the Content Platform Engine application.
deployapplication	deployapplication.xml	Deploys the Content Platform Engine application on the application server.

-taskfile *task_file_name*

The **-taskfile** *task_file_name* parameter specifies the configuration XML file to use.

If only one task file exists for the *task_type*, then the **-taskfile** *task_file_name* parameter is optional.

If more than one task file for the *task_type* exists, then you must include the **-taskfile** *task_file_name* parameter. You can omit the **-task** *task_type* parameter when you specify the **-taskfile** *task_file_name* parameter.

-profile *myprofile*

The **-profile** *myprofile* parameter specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as ce_was_tiv_db2. The profile must be located in the *ce_install_path*/tools/configure/profiles directory, where *ce_install_path* is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2" or /opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2.
- The absolute path to the profile input file, such as "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\

ce_was_tiv_db2\ce_was_tiv_db2.cfg" or /opt/IBM/FileNet/ContentEngine/
tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg".

-silent

The **-silent** parameter is optional. When **-silent** is specified, then no prompts or informational messages are displayed in the console, but the errors are written to the log. Failure messages and validation error messages are displayed as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile, and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force

The **-force** parameter is optional and only applies when the **-silent** parameter is used. When **-force** is specified, then the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help

The **-help** parameter is optional and displays a brief message on the command syntax instead of running the command.

execute command examples

The following examples include line breaks to format the command for reading. Enter the command and options on a single line, without any line breaks.

Run all the tasks in a profile.

The following command runs all the tasks in the wstdb2jdbc profile, which is located in the *ce_install_path/tools/configure/profiles/wstdb2jdbc* directory. If you include the **-silent** parameter in the command, you must also include the **-force** parameter.

```
configmgr_cl execute -profile wstdb2jdbc
```

Run the configurejdbcos task in a profile with one configurejdbcos task.

The following command runs the configurejdbc task in the *ce_install_path/tools/configure/profiles/wstdb2jdbc* directory:

```
configmgr_cl execute -task configurejdbcos -profile wstdb2jdbc
```

Run a single configurejdbcos task in a profile with multiple configurejdbcos tasks:

The following command runs the configurejdbcos.2.xml task file in the *ce_install_path/tools/configure/profiles/wstdb2jdbc* directory:

```
configmgr_cl execute -taskfile configurejdbc.2.xml -profile wstdb2jdbc
```

Display the help for the execute command.

The following command displays the help for the **execute** command:

```
configmgr_cl execute -help
```

generateconfig command

The **generateconfig** command generates the configuration XML file for the specified configuration task. The command name is not case sensitive.

generateconfig command syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line, without any line breaks.

```
configmgr_cl generateconfig -appserver app_server_type  
-repositorytype ldap_repository_type  
-db database_type -ldap ldap_type -bootstrap bootstrap_operation  
-deploy deploy_type -task task_type -taskname display_name  
-profile myprofile [-silent] [-force] [-help]
```

generateconfig command parameters

-appserver *appserver_name*

The **-appserver** *appserver_type* specifies the type of application server and must be WebSphere, WebLogic, or JBoss.

-repositorytype *ldap_repository_type*

WebSphere Application Server only. The **-repositorytype** *ldap_repository_type* parameter is required only when you are generating the XML files. This parameter specifies the type of LDAP repository to use and must be standalone or federated.

-db *database_type*

The **-db** *database_type* parameter is required only when you are generating all the files at the same time or when you are generating a single file by using the configurejdbcgcd or configurejdbcos option. This parameter specifies the type of database to be used by Content Platform Engine and must be mssql, oracle, oracle_rac, db2, or db2zos.

-ldap *ldap_type*

The **-ldap** *ldap_type* parameter is required only when you are generating all the files at the same time or when you are generating a single file by using the configureldap option. This parameter specifies the type of directory service repository that Content Platform Engine uses for authenticating users and must be activedirectory, adam, ca, edirectory, oid, oracledirectoryse, or tivoli. The adam option applies to both Microsoft ADAM and AD LDS.

-bootstrap *bootstrap_operation*

The **-bootstrap** *bootstrap_operation* parameter is required only when you are generating all the files at the same time or when you are generating a single file by using the configurebootstrap option. This parameter specifies the bootstrap and text extraction operation for the profile and must be new, modify, or upgrade.

-deploy *deploy_type*

The **-deploy** *deploy_type* parameter is required only when you are generating all the files at the same time or when you are generating a single file by using the deployapplication option. This parameter specifies the type of Content Platform Engine deployment. The value must be standard, cluster, or netdeploy (network deployment).

Specify standard if you are deploying Content Platform Engine to a stand-alone (that is, a server that is not managed or clustered) WebSphere Application Server, Oracle WebLogic Server, or JBoss Application Server.

Specify cluster if you are deploying Content Platform Engine to a WebSphere Application Server, Oracle WebLogic Server, or JBoss Application Server cluster.

Specify netdeploy if you are deploying Content Platform Engine to a managed WebSphere Application Server instance. That is, you are using Network Deployment to manage individual servers that are not in a cluster.

-task task_type

The **-task task_type** parameter indicates which task to generate. You can omit the **-task task_type** parameter if you want to generate all the tasks. The *task_type* value is not case sensitive. The following table lists the valid task names, the associated configuration XML file, and a description of the Content Platform Engine settings affected by the task.

Table 43. task_type values

Option	Configuration file to generate	Description
omitted	applicationserver.xml	If you omit the -task task_type parameter, then all the default configuration files for a profile are created.
	configurebootstrap.xml	
	configurejdbcgcd.xml	
	configurejdbcos.xml	
	configureldap.xml	
	configureloginmodules.xml	
	deployapplication.xml	
configurebootstrap	applicationserver.xml	Generates the file for the application server properties and the file with the settings for the Content Platform Engine bootstrap on the application server. The bootstrap information is needed for creating the global configuration database and for starting Content Platform Engine.
	configurebootstrap.xml	
configurejdbcgcd	applicationserver.xml	Generates the file for the application server properties and the file with the settings for configuring the JDBC connections to the global configuration database used by Content Platform Engine.
	configurejdbcgcd.xml	
		If the profile already contains an applicationserver.xml file, the existing file is retained.

Table 43. *task_type* values (continued)

Option	Configuration file to generate	Description
configurejdbcos	<p>applicationserver.xml</p> <p>configurejdbcos.xml</p> <p>configurejdbcos.<i>n</i>.xml, where <i>n</i> is an integer starting with 2</p>	<p>Generates the file for the application server properties and the file with the settings for configuring JDBC connections to a single object store database used by Content Platform Engine. You need to generate, edit, and apply the configurejdbcos task settings for each object store in your database.</p> <p>When you generate a second object store JDBC configuration file, it is named configurejdbcos.2.xml. The filename increments for each new file you generate. You cannot change the filename, but you can edit the value in the file for the name of the task.</p> <p>If the profile already contains an applicationserver.xml file, the existing file is retained.</p>
configureldap	<p>applicationserver.xml</p> <p>configureldap.xml</p> <p>configureldap.<i>n</i>.xml, where <i>n</i> is an integer starting with 2</p>	<p>Generates the file for the application server properties and the file for configuring the connection to the directory server for authenticating Content Platform Engine users.</p> <p>(WebSphere Application Server or Oracle WebLogic Server only.) When you generate a second LDAP configuration file, it is named configureldap.2.xml. The filename increments for each new file you generate. You cannot change the filename, but you can edit the value in the file for the name of the task.</p> <p>If the profile already contains an applicationserver.xml file, the existing file is retained.</p>

Table 43. *task_type* values (continued)

Option	Configuration file to generate	Description
configureloginmodules	applicationserver.xml configureloginmodules.xml	(WebSphere Application Server or JBoss Application Server only.) Generates the file for the application server properties and the files for the login modules for the Content Platform Engine application. If the profile already contains an applicationserver.xml file, the existing file is retained.
deployapplication	applicationserver.xml deployapplication.xml	Generates the file for the application server properties and the file with settings for deploying the Content Platform Engine application on the application server. If the profile already contains an applicationserver.xml file, the existing file is retained.

-taskname *display_name*

The **-taskname** *display_name* parameter is optional and is valid only for generating the files. This parameter specifies the value for the `displayName` attribute in the configuration XML file. If the display name includes spaces, put the entire name inside quotation marks. The display name is used in the graphical user interface to identify the task.

-profile *myprofile*

The **-profile** *myprofile* parameter specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as `ce_was_tiv_db2`. The profile must be located in the `ce_install_path/tools/configure/profiles` directory, where `ce_install_path` is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2"` or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2`.
- The absolute path to the profile input file, such as `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg"` or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg`.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg"`.

-silent

The **-silent** parameter is optional. When **-silent** is specified, then no prompts or informational messages are displayed in the console, but the errors are written to the log. Failure messages and validation error messages are displayed as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile, and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force

The **-force** parameter is optional and only applies when the **-silent** parameter is used. When **-force** is specified, then the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help

The **-help** parameter is optional and displays a brief message on the command syntax instead of running the command.

generateconfig command examples

The following examples include line breaks to format the command for reading. Enter the command and options on a single line, without any line breaks.

Generate all configuration files at the same time.

The following command generates all the configuration XML files for a new installation profile for a standard deployment on WebSphere with IBM Tivoli Directory Server that uses a stand-alone LDAP repository and DB2 in the *ce_install_path/tools/configure/profiles/wstdb2* directory:

```
configmgr_cl generateconfig -appserver websphere -repositorytype standalone
-db db2 -ldap tivoli -bootstrap new -deploy standard -profile wstdb2
```

Generate only the configurejdbcos task file for an object store.

The following command generates only the *configurejdbcos.n.xml* file for a new installation profile for deployment on WebSphere that uses a stand-alone LDAP repository in the *ce_install_path/tools/configure/profiles/wstdb2* directory:

```
configmgr_cl generateconfig -appserver websphere -db db2 -repositorytype
standalone -task configurejdbcos -profile wstdb2jdbc
```

Generate only the configurejdbcos task file for an object store and provide a display name for the task.

The following command generates only the *configurejdbcos.n.xml* file for a new installation profile for deployment on WebSphere that uses a stand-alone LDAP repository in the *ce_install_path/tools/configure/profiles/wstdb2* directory and uses a display name of *Configure Object Store OS23 Data Sources*:

```
configmgr_cl generateconfig -appserver websphere -db db2
-repositorytype standalone task configurejdbcos
-taskname "Configure Object Store OS23 Data Sources"
-profile wstdb2jdbc
```

Display the help for the generateconfig command.

The following command displays the help for the **generateconfig** command:

```
configmgr_cl generateconfig -help
```

gui command

The **gui** command opens the Configuration Manager graphical user interface. The command is not case sensitive.

gui command syntax

```
configmgr_cl gui
```

gui command Example

The following command starts the Configuration Manager graphical user interface:

```
configmgr_cl gui
```

listtasks command

The **listtasks** command displays a list of the tasks and the task files in the configuration profile. The command name is not case sensitive.

listtasks command syntax

```
configmgr_cl listtasks [-task task_type] -profile myprofile
[-help]
```

listtasks command parameters

-task *task_type*

The **-task *task_type*** parameter is optional and indicates which task type to list. The *task_type* value is not case sensitive. The following table lists the valid task names, the associated configuration XML file, and a description of the Content Platform Engine settings affected by the task.

Table 44. *task_type* values

Option	Configuration files	Description
omitted	configurebootstrap.xml configurejdbcgcd.xml configurejdbcos.xml configurejdbcos. <i>n</i> .xml configureldap.xml configureldap. <i>n</i> .xml configureloginmodules.xml deployapplication.xml Where <i>n</i> is an integer starting with 2	If you omit the -task <i>task_type</i> parameter, then all the configuration tasks and the associated task files for the profile are listed.
configurebootstrap	configurebootstrap.xml	Lists the task for configuring the settings for the Content Platform Engine bootstrap and text extraction on the application server. The bootstrap information is needed for creating the global configuration database and for starting Content Platform Engine.

Table 44. *task_type* values (continued)

Option	Configuration files	Description
configurejdbcgcd	configurejdbcgcd.xml	Lists the task for configuring the settings for the JDBC connections to the global configuration database used by Content Platform Engine.
configurejdbcos	configurejdbcos.xml configurejdbcos. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Lists the task for configuring the settings for the JDBC connections to a single object store database used by Content Platform Engine. You must generate, edit, and apply the configurejdbcos task settings for each object store in your database. When you generate a second object store JDBC configuration file, it is named configurejdbcos.2.xml. The filename increments for each new file you generate.
configureldap	configureldap.xml configureldap. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Lists the tasks for configuring the connection to the directory server for authenticating Content Platform Engine users. (WebSphere Application Server or Oracle WebLogic Server only) When you generate a second LDAP configuration file, it is named configureldap.2.xml. The filename increments for each new file you generate. When you generate a second LDAP configuration file, it is named configureldap.2.xml. The filename increments for each new file you generate. You cannot change the filename, but you can edit the value in the file for the name of the task.
configureloginmodules	configureloginmodules.xml	(WebSphere Application Server or JBoss Application Server only.) Lists the task for configuring the login modules for the Content Platform Engine application.
deployapplication	deployapplication.xml	Lists the task for deploying the Content Platform Engine application on the application server.

-profile *myprofile*

The **-profile** *myprofile* parameter specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as `ce_was_tiv_db2`. The profile must be located in the `ce_install_path/tools/configure/profiles` directory, where `ce_install_path` is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2"` or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2`.
- The absolute path to the profile input file, such as `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg"` or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg`.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg"`.

-help

The **-help** parameter is optional and displays a brief message on the command syntax instead of running the command.

listtasks command examples

List all the configuration tasks in the profile.

The following command lists all the configuration tasks and the associated configuration XML files in the `wstdb2` profile located in the `ce_install_path/tools/configure/profiles/wstdb2` directory:

```
configmgr_cl listtasks -profile wstdb2
```

A message like the following example is displayed:

All tasks in profile `wstdb2`. The tasks will be executed in the positions indicated when executing all tasks:

Task 1:

Name: Configure GCD JDBC Data Sources
Type: `configurejdbcgcd`
File: `configurejdbcgcd.xml`

Task 2:

Name: Configure Object Store JDBC Data Sources
Type: `configurejdbcos`
File: `configurejdbcos.xml`

Task 3:

Name: Configure Login Modules
Type: `configureloginmodules`
File: `configureloginmodules.xml`

Task 4:

Name: Configure LDAP
Type: `configureldap`
File: `configureldap.xml`

Task 5:

Name: Configure Bootstrap and Text Extraction
Type: `configurebootstrap`
File: `configurebootstrap.xml`

Task 6:

Name: Deploy Application
Type: `deployapplication`
File: `deployapplication.xml`

List all the configurejdbcos tasks in the profile.

The following command lists all the configure JDBC settings for the object store tasks and the associated configuration XML files in the wstdb2 profile located in the *ce_install_path/tools/configure/profiles/wstdb2* directory:

```
configmgr_cl listtasks -task configurejdbcos -profile wstdb2
```

A message like the following example is displayed:

```
Tasks in profile wstdb2 of the task type configurejdbcos:
Task name: Configure Object Store JDBC Data Sources
File: configurejdbcos.xml
```

Display the help for the listtasks command.

The following command displays the help for the **listtasks** command:

```
configmgr_cl listtasks -help
```

movetask command

The **movetask** command moves a task to a different position in the list of tasks. The task position determines the order that the tasks are run when you run all the tasks at the same time. You use the **listtask** command to display the task order. The command names are not case sensitive.

movetask command syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line, without any line breaks.

```
configmgr_cl movetask -task task_type | -taskfile task_file_name
-position new_position -profile myprofile [-silent][-force][-help]
```

movetask command parameters

-task *task_type*

The **-task** *task_type* parameter indicates which task to move. This parameter must be included if the **-taskfile** *task_file_name* parameter is omitted. The *task_type* value is not case sensitive. The following table lists the valid task names, the associated configuration XML file, and a description of the Content Platform Engine settings affected by the task.

Table 45. *task_type* values

Option	Configuration files	Description
configurebootstrap	configurebootstrap.xml	Moves the task for configuring the settings for the Content Platform Engine bootstrap and text extraction on the application server. The bootstrap information is needed for creating the global configuration database and for starting Content Platform Engine
configurejdbcgcd	configurejdbcgcd.xml	Moves the task for configuring the settings for the JDBC connections to the global configuration database used by Content Platform Engine.

Table 45. *task_type* values (continued)

Option	Configuration files	Description
configurejdbcos	configurejdbcos.xml configurejdbcos. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Moves the task for configuring the settings for the JDBC connections to a single object store database used by Content Platform Engine. When you generate a second object store JDBC configuration file, it is named configurejdbcos.2.xml. The filename increments for each new file you generate.
configureldap	configureldap.xml configureldap. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Moves the task for configuring the connection to the directory server for authenticating Content Platform Engine users. (WebSphere Application Server or Oracle WebLogic Server only) When you generate a second LDAP configuration file, it is named configureldap.2.xml. The filename increments for each new file you generate. When you generate a second LDAP configuration file, it is named configureldap.2.xml. The filename increments for each new file you generate.
configureloginmodules	configureloginmodules.xml	Moves the task for configuring the login modules for the Content Platform Engine application.
deployapplication	deployapplication.xml	Moves the task for deploying the Content Platform Engine application on the application server.

-taskfile *task_file_name*

The **-taskfile** *task_file_name* parameter specifies the configuration XML file to use.

If only one task file exists for the *task_type*, then the **-taskfile** *task_file_name* parameter is optional.

If more than one task file for the *task_type* exists, then you must include the **-taskfile** *task_file_name* parameter. You can omit the **-task** *task_type* parameter when you specify the **-taskfile** *task_file_name* parameter.

-position*new_position*

The **-position***new_position* parameter specifies the new position in the list for the item. You can run the **listtasks** to view the list of tasks in the profile and their position before you run the **movetask** command.

-profile *myprofile*

The **-profile** *myprofile* parameter specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as `ce_was_tiv_db2`. The profile must be located in the `ce_install_path/tools/configure/profiles` directory, where `ce_install_path` is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as "`C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2`" or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2`.
- The absolute path to the profile input file, such as "`C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg`" or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg`.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter "`C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg`".

-silent

The **-silent** parameter is optional. When **-silent** is specified, then no prompts or informational messages are displayed in the console, but the errors are written to the log. Failure messages and validation error messages are displayed as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile, and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force

The **-force** parameter is optional and only applies when the **-silent** parameter is used. When **-force** is specified, then the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help

The **-help** parameter is optional and displays a brief message on the command syntax instead of running the command.

movetask command examples

Move the task for the configurejdbcos.3.xml file in a profile with more than one configurejdbcos task.

The following command moves the task for the `configurejdbcos.3.xml` file for the `wstdb2` profile located in the `ce_install_path/tools/configure/profiles/wstdb2` directory to position 1:

```
configmgr_cl movetask -taskfile configurejdbcos.3.xml -position 1
-profile wstdb2
```

Move the configureloginmodules task.

The following command moves the `configureloginmodules` task from the default position of task 3 to task 5 in the `wstdb2` profile located in the `ce_install_path/tools/configure/profiles/wstdb2` directory:

```
configmgr_cl movetask -task configureloginmodules -position 5
-profile wstdb2
```

Display the help for the movetask command.

The following command displays the help for the **movetask** command:

```
configmgr_cl movetask -help
```

removetask command

The **removetask** command removes the specified task from the configuration profile. When you remove the task, the configuration XML file is deleted from the profile directory. The command name is not case sensitive.

removetask command syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line, without any line breaks.

```
configmgr_cl removetask -task task_type | -taskfile task_file_name  
-profile myprofile [-silent][-force][-help]
```

removetask command parameters

-task *task_type*

The **-task** *task_type* parameter is optional and indicates which task to remove. You can omit the **-task** *task_type* parameter if you specify the **-taskfile** *task_file_name* parameter. The *task_type* value is not case sensitive. The following table lists the valid task names, the associated configuration XML file, and a description of the Content Platform Engine settings affected by the task.

Table 46. *task_type* values

Option	Configuration file to remove	Description
configurebootstrap	configurebootstrap.xml	Settings for the Content Platform Engine bootstrap and text extraction on the application server. The bootstrap information is needed for creating the global configuration database and for starting Content Platform Engine.
configurejdbcgcd	configurejdbcgcd.xml	Settings for configuring the JDBC connections to the Content Platform Engine database used by Content Platform Engine.

Table 46. *task_type* values (continued)

Option	Configuration file to remove	Description
configurejdbcos	configurejdbcos.xml configurejdbcos. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Settings for configuring JDBC connections to a single object store database used by Content Platform Engine. You need to generate, edit, and apply the configurejdbcos task settings for each object store in your database. If you generate a second object store JDBC configuration file, then it is named configurejdbcos.2.xml. The filename increments for each new file you generate.
configureldap	configureldap.xml configureldap. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Configures the connection to the directory server for authenticating Content Platform Engine users. (WebSphere Application Server or Oracle WebLogic Server only) If you generate a second LDAP configuration file, then it is named configureldap.2.xml. The filename increments for each new file you generate. If your profile contains more than one configureldap task, then you must specify the -taskfile <i>task_file_name</i> parameter to identify the task to remove.
configureloginmodules	configureloginmodules.xml	(WebSphere Application Server or JBoss Application Server only) Creates the login modules for the Content Platform Engine application.
deployapplication	deployapplication.xml	Deploys the Content Platform Engine application on the application server.

-taskfile *task_file_name*

The **-taskfile** *task_file_name* parameter specifies the configuration XML file to use.

If only one task file exists for the *task_type*, then the **-taskfile** *task_file_name* parameter is optional.

If more than one task file for the *task_type* exists, then you must include the **-taskfile** *task_file_name* parameter. You can omit the **-task** *task_type* parameter when you specify the **-taskfile** *task_file_name* parameter.

-profile *myprofile*

The **-profile** *myprofile* parameter specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as `ce_was_tiv_db2`. The profile must be located in the `ce_install_path/tools/configure/profiles` directory, where `ce_install_path` is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2"` or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2`.
- The absolute path to the profile input file, such as `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg"` or `/opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg`.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter `"C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg"`.

-silent

The **-silent** parameter is optional. When **-silent** is specified, then no prompts or informational messages are displayed in the console, but the errors are written to the log. Failure messages and validation error messages are displayed as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile, and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force

The **-force** parameter is optional and only applies when the **-silent** parameter is used. When **-force** is specified, then the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help

The **-help** parameter is optional and displays a brief message on the command syntax instead of running the command.

removetask command examples

Remove the configurejdbcos task from a profile with only one configurejdbcos task.

The following command removes the `configurejdbcos` task and the `configurejdbcos.xml` file from the profile named `wstdb2jdbc_one`.

```
configmgr_cl removetask -task configurejdbcos -profile wstdb2jdbc_one
```

Remove the configurejdbcos task from a profile with several configurejdbcos tasks.

The following command removes the `configurejdbcos` task and the `configurejdbcos.2.xml` file from the profile named `wstdb2jdbc_many`.

```
configmgr_cl removetask -taskfile configurejdbcos.2.xml  
-profile wstdb2jdbc_many
```

Remove the configurejdbcos task from a profile with several configurejdbcos tasks by using an absolute path to the profile directory.

The following command removes the `configurejdbcos` task and the `configurejdbcos.2.xml` file from the profile named `wstdb2jdbc_many` that is located in the `c:\temp\myprofiles\wstdb2jdbc_many` directory.

```
configmgr_cl removetask -taskfile configurejdbcos.2.xml
-profile c:\temp\myprofiles\wstdb2jdbc_many
```

Display the help for the removetask command.

The following command displays the help for the **removetask** command:

```
configmgr_cl removetask -help
```

storepasswords command

The **storepasswords** command prompts for passwords that are blank in a profile and stores the encrypted passwords in the file. Storing encrypted passwords might not be FIPS 140-2 compliant. You can run the command for a single task or for all tasks in the profile. The command name is not case sensitive.

storepasswords command syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line, without any line breaks.

Tip: If the **storepasswords** command prompts you to store passwords in configuration files on disk, you must respond with yes or no (instead of y or n).

```
configmgr_cl storepasswords [-task task_type | -taskfile task_file_name]
-profile myprofile [-help]
```

storepasswords command parameters

-task task_type

The **-task task_type** parameter specifies a specific task to encrypt passwords for. You can omit the **-task task_type** parameter if you want to store passwords for all the tasks or if you specify the **-taskfile task_file_name** parameter. The *task_name* value is not case sensitive. The following table lists the valid task names, the associated configuration XML file, and a description of the Content Platform Engine settings affected by the task.

Table 47. task_type values

Option	Configuration file	Description
omitted	applicationserver.xml	If you omit the <code>-task <i>task_type</i></code> parameter and the <code>-taskfile <i>task_file_name</i></code> parameter, then you are prompted to enter the passwords for each configuration XML file in the profile. Each password is encrypted before it is added to the XML file.
	configurebootstrap.xml	
	configurejdbcgcd.xml	
	configurejdbcos.xml	
	configurejdbcos. <i>n</i> .xml	
	configureldap.xml	
	configureldap. <i>n</i> .xml	
	deployapplication.xml	
	Where <i>n</i> is an integer starting with 2	

Table 47. *task_type* values (continued)

Option	Configuration file	Description
configurebootstrap	configurebootstrap.xml	Encrypts the password for the BootstrapPassword property that is used to create the global configuration database and to start Content Platform Engine.
configurejdbcgcd	configurejdbcgcd.xml	Encrypts the password for the DatabasePassword property that Content Platform Engine uses to access the GCD database.
configurejdbcos	configurejdbcos.xml configurejdbcos. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Encrypts the password for the DatabasePassword property that Content Platform Engine uses to access the object store database. If you have more than one configurejdbcos. <i>n</i> .xml file, run the command for each task file.

-taskfile *task_file_name*

The **-taskfile** *task_file_name* parameter specifies the configuration XML file to use.

If only one task file exists for the *task_type*, then the **-taskfile** *task_file_name* parameter is optional.

If more than one task file for the *task_type* exists, then you must include the **-taskfile** *task_file_name* parameter. You can omit the **-task** *task_type* parameter when you specify the **-taskfile** *task_file_name* parameter.

-profile *myprofile*

The **-profile** *myprofile* parameter specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as ce_was_tiv_db2. The profile must be located in the *ce_install_path*/tools/configure/profiles directory, where *ce_install_path* is the location where the Content Platform Engine software is installed.
- The absolute path to the profile directory, such as "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2" or /opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2.
- The absolute path to the profile input file, such as "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg" or /opt/IBM/FileNet/ContentEngine/tools/configure/profiles/ce_was_tiv_db2/ce_was_tiv_db2.cfg.

Remember: If the path includes a directory name with spaces, enclose the entire path in quotation marks. For example, enter "C:\Program Files\IBM\FileNet\ContentEngine\tools\configure\profiles\ce_was_tiv_db2\ce_was_tiv_db2.cfg".

storepasswords command examples

Encrypt and save all passwords for a profile.

The following command encrypts and saves passwords for any blank entries in the profile named wstdb2jdbc_one.

```
configmgr_cl storepasswords -profile wstdb2jdbc_one
```

Encrypt and save the passwords for a specific configurejdbcos task in a profile with several configurejdbcos tasks.

The following command encrypts and saves passwords for any blank entries in the configurejdbcos.2.xml file from the profile named wstdb2jdbc_many.

```
configmgr_cl storepasswords -taskfile configurejdbcos.2.xml  
-profile wstdb2jdbc_many
```

Display the help for the storepasswords command.

The following command displays the help for the **storepasswords** command:

```
configmgr_cl storepasswords -help
```

Appendix B. Troubleshooting FileNet P8 installation and upgrade

This section provides troubleshooting solutions for problems you might encounter when installing or upgrading FileNet P8 software.

“Application server does not start after installation and shutdown (WebSphere Application Server)”

The WebSphere Application Server might not start after installation and shutdown because LDAP settings are not configured correctly or JVM startup arguments are not specified properly.

“Changing an incorrect value for the .NET API COM Compatibility Layer (CCL) server URL” on page 204

If you specified an incorrect value for the .NET API COM Compatibility Layer (CCL) server URL during Content Platform Engine installation, you cannot correct the URL by using Configuration Manager to edit the dotnetclient configuration profile.

Application server does not start after installation and shutdown (WebSphere Application Server)

The WebSphere Application Server might not start after installation and shutdown because LDAP settings are not configured correctly or JVM startup arguments are not specified properly.

Symptoms

The WebSphere Application Server does not start after installation and shutdown.

Causes

This problem can occur because of several reasons:

- After you enable Global Security, the WebSphere Application Server might not be able to start because LDAP repository settings are not configured correctly. This condition is more likely to happen if you use Standalone as your default LDAP repository.
- You specified incorrect JVM startup arguments.

Resolving the problem

To resolve the LDAP problem, you must have valid LDAP users to enable Global Security.

Important: The WebSphere Application Server User ID (referred to as the WebSphere Administrative Login during Content Engine installation) must reside within the LDAP Base Distinguished Name that you specified during Content Engine installation.

To modify your LDAP settings:

1. Run `IBM\WebSphere\AppServer\profiles\profile\bin\wsadmin -conntype NONE`.
2. At the `wsadmin>` prompt, enter `securityoff`.
3. Enter `exit`.
4. Restart the application server.

5. Start the WebSphere Console and make the necessary changes to the LDAP security settings.
6. In the WebSphere Console, re-enable Global Security.

To correct the JVM startup arguments, modify or remove the problematic argument values:

1. Open the `/IBM/WebSphere/AppServer/profiles/<profile>/config/cells/<cell_name>/nodes/<node_name>/servers/<server_name>/servers.xml` file.
2. Search for "genericJvmArguments".
3. Modify or remove the incorrect argument values.
4. Save your changes.

Changing an incorrect value for the .NET API COM Compatibility Layer (CCL) server URL

If you specified an incorrect value for the .NET API COM Compatibility Layer (CCL) server URL during Content Platform Engine installation, you cannot correct the URL by using Configuration Manager to edit the dotnetclient configuration profile.

Symptoms

An incorrect .NET API COM Compatibility Layer (CCL) server URL was entered during software installation.

Resolving the problem

Correct the URL by taking the following steps.

Changing the .NET API COM Compatibility Layer (CCL) server URL

1. Open the `configmgr.properties` file for editing. This file is located in the path `ce_install_path/tools/configure/configuration/`. Find the line in the file that starts with `CCL_URL` and replace the URL with the correct value:

2. Find the line in the file that starts with `CCL_URL`

```
CCL_URL=http://localhost:port_number/wsi/FNCEWS40MTOM/
```

and replace the URL with the correct value.

3. Run Configuration Manager to reexecute the dotnetclient profile (which the Content Platform Engine installation program automatically ran when it installed Content Platform Engine). You can reexecute the profile using either the graphical user interface. Or you can reexecute the profile using the command-line interface:

```
configmgr_cl execute -task configureDotNetAPI -profile dotnetclient
```

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy,

modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com)[®] are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol ([®] or [™]), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml> (www.ibm.com/legal/copytrade.shtml).

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Other company, product, and service names may be trademarks or service marks of others.

Index

A

- Application Engine
 - access roles 107
 - administrator access roles 107
 - administrators 107
 - Application Name 110
 - configuring on all application servers 91
 - configuring on WebSphere 92
 - configuring SSL 117
 - container-managed authentication on WebSphere 93
 - deploying on all application servers 103
 - deploying on WebSphere 104
 - deploying on WebSphere 7.0 105
 - indexing 110
 - installing 84
 - installing and configuring 83
 - installing Content Platform Engine Client 89
 - installing interactively 85
 - installing silently 86
 - installing software updates 89
 - multiple instances 127, 128
 - removing ISRA servlet 147
 - removing on WebSphere 143
 - setting up full SSL support 118
- Application Integration
 - installing 125
 - installing interactively 125
 - installing silently 126
 - verify installation 127
- authentication token
 - IBM Content Search Services server 70

B

- banner image
 - changing 107
- bootstrap preferences
 - configuring 107
 - enhanced time zone 111
 - setting on first login 107
 - setting the SSL configuration for Application Engine 107
- bootstrap properties 171
- bootstrap.properties file
 - sharing between Application Engines 119

C

- CA certificates
 - deploying on Content Platform Engine 80
- certificates
 - validating on IBM Content Search Services 81

- checkstatus command 178
- COM compatibility layer 134
- COM compatibility layer (CCL)
 - installing 134
- configmgr.ini 176
- configuration
 - IBM Content Search Services 69
- configuration and startup tasks 113
- Configuration Manager
 - config_mgr_user* permissions 18
 - adding an SSL signer to the keystore 157, 158
 - adding new tasks 174
 - applying configuration settings from the command line 38, 39
 - applying the bootstrap and text extraction properties settings 173
 - applying the Configure JDBC Data Sources settings 172
 - applying the property settings in a task 172
 - changing password preference for installation 20
 - checking the completion status of a task from the command line 41
 - checking the completion status of all configuration tasks from the command line 42
 - checking the completion status of one configuration task from the command line 42
 - checking the status of a task 175
- checkstatus command 178
- command line interface 27
- command-line reference 176
- configure bootstrap and text extraction settings by using the GUI 26
- configuring Content Platform Engine using the graphical user interface 19
- console toolbar 161
- creating a new profile 167
- creating an upgrade profile 167
- delete task 174
- deploying Content Platform Engine 173
- editing a configuration XML file for installation 34
- editing a task 169
- editing the application server properties 169
- editing the Configure Bootstrap and Text Extraction Properties task 171
- editing the Configure JDBC Data Sources task 170
- editing the Configure LDAP task 170
- editing the Deploy Application task 171
- execute command 182
- generateconfig command 186

- Configuration Manager (*continued*)
 - generating a configuration XML file for installation (WebSphere) 31
 - generating all of the configuration XML files at the same time 29
 - grant user permissions 18
 - graphical user interface and command-line interface differences 154
 - gui command 191
 - GUI reference 159
 - Installation and Upgrade Worksheet 155
 - listtasks command 191
 - logs 156
 - main toolbar 160
 - menus and commands 162
 - movetask command 194
 - new profile 21
 - opening an existing profile 168
 - overview 151, 152
 - passwords 155
 - profile concepts 152
 - profile toolbar 161
 - reference 151
 - removetask command 197
 - running a selected task 175
 - running all configuration XML files at the same time 38
 - running all tasks at the same time 175
 - running commands 177
 - running configuration XML files for installation 37
 - running configuration XML files one at a time 39
 - saving changes to a task or profile 176
 - setting password save preference 166
 - starting 20
 - starting for installation 159
 - storepasswords command 200
 - task status 175
 - viewing the session log 176
 - window description 160
 - working in the Configuration Manager window 160
 - working with 165
- configuration profile
 - adding new tasks 174
 - creating a new profile 21
 - renaming tasks 174
- configuration tasks
 - adding 174
 - renaming 174
- configuration XML files
 - applying installation settings in Configuration Manager 37
 - configure bootstrap and text extraction settings by using the Configuration Manager GUI 26

- Configure global configuration database (GCD) data source 22
- Configure LDAP 173
- Configure LDAP task
 - using the Configuration Manager GUI 25
- Configure Login Modules 172
- Configure Login Modules task (for WebSphere and JBoss only) 24
- configuring Content Platform Engine 17, 18
- configuring Content Platform Engine using the Configuration Manager graphical user interface 19
- configuring environment variables 52
- connection point
 - configure for Application Engine 113
- container-managed authentication
 - Application Engine on WebSphere 93
- content based retrieval
 - enabling index objects for 74
- Content Engine
 - using command line interface to configure 27
- Content Platform Engine
 - configuration IBM Content Search Services servers on Content Platform Engine 71
 - configure bootstrap and text extraction settings by using the Configuration Manager GUI 26
 - Configure LDAP task 25
 - configuring 17, 18
 - configuring an instance 166
 - configuring file stores 54
 - configuring for IBM Content Search Services 70
 - configuring IBM Content Search Services servers 71
 - configuring login modules (WebSphere and JBoss only) 24
 - connecting
 - load balancer 62
 - correcting a dotnetclient configuration profile error 156
 - creating a database connection 58
 - creating a profile by using the command line 28
 - creating a workflow system 60
 - deploying CA certificates 80
 - deploying instances 44
 - deploying instances using the GUI 44
 - deploying on server clusters 61
 - generating configuration XML files by using the Configuration Manager command line 28
 - highly available connection 60
 - installing 11
 - installing and configuring 9
 - installing interactively 12
 - installing silently 13
 - installing software updates 14
 - login modules 170
 - post deployment steps 54
 - post-deployment steps
 - WebSphere 54

- Content Platform Engine (*continued*)
 - removing 139
 - removing data 139
 - removing interactively on AIX, HP/UX, Linux, Linux for System z 139
 - removing silently 139
 - self-signed certificates 80
 - setting the indexing languages 71
 - Solaris 139
 - SSL signer error 157, 158
 - storage device source files 50
 - third party certificates 80
 - verify installation 62
 - verifying deployment 55
 - web service 114, 115
- Content Platform Engine Client
 - installing interactively on Application Engine 89
 - installing on Application Engine 89
 - installing silently on Application Engine 90
- Content Platform Engine Web Service Transport
 - connecting to Content Platform Engine 62
- creating a database connection 58
- creating a new profile
 - Configuration Manager 167
- creating a workflow system 60
- creating an object store 59
- creating an upgrade profile
 - Configuration Manager 167

D

- data source
 - global configuration database (GCD) 22
- data sources
 - creating by using the Configuration Manager command line 33
- delete task 174
- deploy application 171
- deploy application task
 - checking the configuration status of 49
- deployapplication.xml file
 - generating 46
 - running 48
- deploying Content Platform Engine using the command line 45
- deployment configuration files
 - editing 47
- document
 - check in (verify new object store) 62
 - check out (verify new object store) 62
 - create (verify new object store) 62
- documentation
 - configuring site preference settings for 107
 - installing as a local information center 3
 - installing information center interactively 4
 - removing from WebSphere Application Server 137

- documentation (*continued*)
 - starting 6
 - verifying 6
- domain
 - users group 59
- domain, FileNet P8 58
 - create 58

E

- editing a configuration XML file 34
- editing login modules for Content Platform Engine 170
- EJB transport 114, 115
- EMC Centra SDK 52
- EMC Centra SDK library files
 - installing 51
 - installing for use with Content Platform Engine 51
- enabling text search on object stores 73
- Enterprise Manager
 - enable SSL 117
 - installing 13
- execute command 182

F

- file storage area
 - specify 59
- file stores
 - configuring 54
- FileNet Deployment Manager 123
- FileNet P8
 - backing up 6
 - disaster recovery 6
 - installing 1
 - redeploying 6
 - removing documentation 137
 - removing documentation from WebSphere Application Server 137
 - removing software 135
- FileNet P8 documentation
 - installing 3
- FileNet P8 information center
 - installing 3
 - installing, silently 5

G

- generateconfig command 186
- generating a configuration XML file 31
- generating all of the configuration XML files at the same time 29
- generating configuration XML files 28
- gui command 191

H

- host validation
 - configuring for IBM Content Search Services 82
- how to read syntax diagrams 178

I

- IBM Case Foundation
 - installing 15
 - installing interactively 15
 - installing silently 16
- IBM Content Search Services
 - authentication token 70
 - configuring 65, 69
 - configuring Content Platform Engine 70
 - configuring for Content Platform Engine 69
 - configuring host validation 82
 - configuring SSL for 76
 - creating index areas 72
 - deploying server certificates 78
 - enabling SSL 77
 - enabling SSL ports 77
 - installing 65, 66
 - installing interactively 67
 - installing silently 68
 - performing server authentication 78
 - removing 141
 - removing interactively 141
 - removing silently 141
 - self-signed certificates 78
 - starting services 68
 - stopping services 68
 - third party certificates 78
 - uninstalling interactively 141
 - validating certificates 81
- IBM Content Search Servicesverifying the installation 75
- IBM FileNet P8 System Health page 55
- IBM Legacy Content Search Engine
 - decommissioning 73
 - disabling 73
- IBM System Dashboard for Enterprise Content Management 134
- IIOP protocol 114, 115
- Image Services library documents 134
- index areas
 - creating 72
- index objects
 - enabling for content based retrieval 74
- information center
 - backing up 6
 - installing 3
 - installing interactively 4
 - redeploying 6
 - starting 6
 - verifying 6
- installation
 - distributed server system 1
 - IBM Content Search Services 65, 66
 - optional tasks 123
 - P8 documentation silent 5
 - troubleshooting 203
- Installing Content Platform Engine 10
- Installing IBM Case Manager 10
- installing silentlyContent Platform Engine 13
- interactive installationIBM Content Search Services 67

- interactive uninstallationIBM Content Search Services 141
- IP address
 - Application Engine SSL host 118
- ISRA
 - installing the servlet 131
 - SSL configurations 131

J

- Java Virtual Machine settings on Application Engine WebSphere 98
- JDBC data source
 - global configuration database (GCD) 22

K

- Kerberos 114, 115

L

- LDAP
 - federated repositories on WebSphere 102
 - Image Services login 133
 - stand-alone on WebSphere 101
- listtasks command 191
- log files
 - Configuration Manager 156
- login modules for Content Platform Engine 24
- LTPA
 - configuring on Application Engine 99

M

- Microsoft Office
 - installing application integration for 125
- movetask command 194
- multi-server configuration
 - Application Engine 127, 128

O

- object store 59
 - data sources 23, 33
 - setting the index languages 71
 - verify new 62
- object store data sources
 - configuring by using the Configuration Manager GUI 23

P

- password preference 166
- passwords
 - Configuration Manager 155
- profile 152
- publishing capabilities 123

R

- realm
 - configuring more than one 120
 - object store administrator 59
- removetask command 197
- Rendition Engine 123
- removing 145

S

- saving passwords to file in Configuration Manager 20
- secure ports
 - enabling on IBM Content Search Services 77
- security
 - setting up SSL for Application Engine 117
 - SSL for Content Engine 115
 - SSL preference setting for Application Engine 107
 - SSL, set up for Content Platform Engine 114
- self-signed certificates
 - deploying on Content Platform Engine 80
 - deploying on IBM Content Search Services 78
- server authentication
 - performing 78
- server certificates
 - deploying on IBM Content Search Services 78
- setting the indexing languages for an object store 71
- silent installation
 - IBM Content Search Services 68
- Site preference settings
 - documentation URL 107
 - name and location 107
- site preferences
 - ISRA 133
 - single index for Application Name 110
- SSL
 - adding an SSL signer to the keystore 157
 - configuring for IBM Content Search Services 76
 - correcting SSL Signer Exchange Prompt errors 158
 - enabling 117
 - enabling for Content Platform Engine 115
 - full support on Application Engine 118
 - Java applets 120
 - security info preference 107
 - setting up for Application Engine 117
 - setting up for Content Platform Engine 114
- SSL ports
 - enabling on IBM Content Search Services 77

SSO

- configuring for Application Engine on WebSphere 95
- start services
 - IBM Content Search Services 68
- stop services
 - IBM Content Search Services 68
- storage device source files 50
- storepasswords command 200
- subfolder, create, (verify new object store) 62
- syntax diagrams 178

T

- T3 protocol 114
- T3protocol 115
- text extraction 171
- text search on object stores
 - enabling 73
- third party certificates
 - deploying on Content Platform Engine 80
 - deploying on IBM Content Search Services 78
- Tivoli Storage Manager
 - adding native API library paths WebSphere 50
- Tivoli Storage Manager (WebSphere Application Server)
 - installing client and adding native API library paths 50
- Tivoli Storage Manager API libraries
 - copying to additional servers 50
- Tivoli Storage Manager client
 - installing 50
- Tivoli Storage Manager native API library files
 - creating a shared library definition 51
- troubleshooting
 - application server does not start 203
 - application server problems
 - troubleshooting 203
 - changing .NET API CCL URL 204
 - Content Platform Engine 204
 - installation 203
 - upgrade 203

U

- upgrade
 - troubleshooting 203
- upgrade profile
 - Configuration Manager 167
- User Token
 - configuring 107

V

- verification
 - IBM Content Search Services
 - installation 75
- verifying Content Platform Engine deployment 55

W

- WAR or EAR file
 - re-creating on WebSphere 105
- web services
 - Content Platform Engine 114, 115
 - Process Engine 115
- WebSphere
 - configuring Application Engine 92
 - deploying Application Engine 104
- workflow subscription wizard 110
- Workplace
 - Application Integration collocation issues 125
 - configuring SSL access to 117
 - defining workflow features for users 120
 - deploying a second instance 128
 - deploying additional instances as an EAR file 129
 - designing publishing templates for users 120
 - designing searches for users 120
 - enable access to tasks and work items 113
 - enable for access to IS documents 130
 - installing Application Integration 125
 - setting bootstrap properties 107
 - setting documentation server URL 107
 - specifying Application Engine administrators 107
 - updating settings
 - load balanced environment 111



Product Number: 5724-R76
5724-R81

GC19-3950-00

