

IBM FileNet P8 Platform
Version 4.5.1

Installation and Upgrade Guide



IBM FileNet P8 Platform
Version 4.5.1

Installation and Upgrade Guide



Note

Before using this information and the product it supports, read the information in "Notices" on page 595.

This edition applies to version 4.5.1 of IBM FileNet Content Manager (product number 5724-R81), version 4.5.1 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, 2010.**

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

Contents

ibm.com and related resources xiii

How to send your comments xiii

Contacting IBM. xiv

Part 1. Installing and configuring IBM FileNet P8 Platform 1

Installing IBM FileNet P8 Platform documentation 3

Before you install the ecm_help documentation package 4

Installing the core IBM FileNet P8 Platform documentation. 4

Installing and re-indexing expansion-products, custom, and auxiliary documentation 6

Starting and verifying the IBM FileNet P8 documentation Web application 9

Backing up and redeploying the FileNet P8 documentation. 9

Installing and configuring Content Engine 11

Installing Content Engine and related client software 12

 Installing Content Engine. 13

 Installing Content Engine interactively 14

 Installing Content Engine silently 14

 Installing Enterprise Manager 15

 Installing Content Engine software updates. . . 16

 Installing the latest Content Search Engine Client files on Content Engine servers. 17

 Installing Content Search Engine Client files interactively 17

 Installing Content Search Engine Client files silently 18

 Installing the latest Process Engine Client files on Content Engine servers 19

 Installing the latest Process Engine Client files on Content Engine servers interactively . . . 19

 Installing the latest Process Engine Client files on Content Engine servers silently. 20

Configuring Content Engine. 21

 Resolving the names of existing data sources . . 22

 Granting directory permissions to the Configuration Manager user. 23

 Configuring Content Engine instances 23

 Configuring Content Engine instances by using the graphical user interface 24

 Starting the Configuration Manager graphical user interface 25

 Changing the password save preference. . 26

 Creating a new configuration profile . . . 26

 Configuring the Global Configuration Data JDBC data source settings 27

 Configuring the login modules (WebSphere and JBoss only) 28

 Configuring the directory service provider (LDAP) settings 29

 Configuring the bootstrap settings. . . . 30

 Configuring instances by using the command line 32

 Generating the configuration XML files for a Content Engine instance 32

 Editing the configuration XML files for a Content Engine instance 39

 Running the configuration XML files . . . 42

 Checking the completion status of Content Engine configuration tasks 46

 Deploying Content Engine instances 48

 Deploying instances by using the graphical user interface 49

 Deploying Content Engine by using the Configuration Manager command line 50

 Generating the deployapplication.xml file . . 51

 Editing the deployment configuration files . . 52

 Running the deployapplication.xml file . . . 53

 Checking the configuration status of the deployapplication task 53

 Deploying Content Engine to additional JBoss servers in a cluster 54

 Installing storage device source files 55

 Installing Tivoli Storage Manager client and adding native API library paths (WebSphere) . . . 55

 Installing Tivoli Storage Manager client . . . 55

 Copying the Tivoli Storage Manager API libraries to additional servers 56

 Creating a shared library definition for Tivoli Storage Manager native API library files. 56

 Installing Tivoli Storage Manager client and adding native API library paths (WebLogic) . . . 56

 Installing Tivoli Storage Manager client . . . 57

 Copying the Tivoli Storage Manager API library files to additional servers 57

 Creating a shared library definition for Tivoli Storage Manager native API library files. 57

 Installing Tivoli Storage Manager client and adding native API library paths (JBoss) 59

 Installing Tivoli Storage Manager client . . . 60

 Copying the Tivoli Storage Manager API libraries to additional servers 60

 Creating a shared library definition for Tivoli Storage Manager native API library files. 60

 Installing or updating EMC Centera SDK library files 61

 Installing EMC Centera SDK version 3.2 library files 62

 Configuring EMC Centera SDK environment variables for version 3.2 63

 Completing Content Engine post-deployment steps 65

Completing Content Engine post-deployment steps (WebSphere)	66
Completing Content Engine post-deployment steps (Oracle WebLogic Server).	67
Completing Content Engine post-deployment steps (JBoss Application Server)	67
Verifying the Content Engine deployment	67
Establishing the FileNet P8 domain and Global Configuration Data (GCD)	69
Creating the data sources for an object store	71
Creating the initial object store data sources by using the graphical user interface	71
Creating additional object store data sources by using the graphical user interface	73
Creating the data sources by using the command line	74
Creating the initial object store	76
Verifying the Content Engine installation	77

Installing and configuring Content Search Engine 79

Installing Content Search Engine	79
Overview	80
Installing Content Search Engine (UNIX)	81
Installing Content Search Engine interactively (UNIX)	81
Installing Content Search Engine silently (UNIX)	83
Starting or stopping the Autonomy K2 services (UNIX)	85
Installing Content Search Engine (Windows)	85
Installing Content Search Engine interactively (Windows).	86
Installing Content Search Engine silently (Windows).	87
Setting the logon user for the K2 Administration Server service (Windows)	87
Configuring Content Search Engine	88
Configuring services on Administration Servers (optional) Installing additional locales	93
Installing additional locales (UNIX)	93
Installing additional locales (Windows)	95
Creating a Content Search Engine collections directory	96
Collections directory requirements.	96
Configuring Content Engine for content-based retrieval	98
Enabling additional K2 index servers and search servers	100
Verifying the Content Search Engine installation	101

Installing and configuring Process Engine 103

Installing Process Engine	103
Verifying the Process Engine database connection	104
Verifying the Process Engine database connection (Oracle)	104
Verifying the Process Engine database connection (SQL Server).	105

Verifying the Process Engine database connection (DB2)	106
Installing Process Engine interactively	106
Installing the Process Engine software interactively (Windows)	107
Installing the Process Engine software interactively (UNIX)	107
Installing Process Engine silently	108
Installing the Process Engine software silently (Windows)	109
Installing the Process Engine software silently (UNIX)	109
Encrypting passwords for Process Engine	110
Resetting administrative user passwords	111
Setting the f_maint and f_sw passwords (Oracle and Microsoft SQL Server)	112
Setting the f_maint and f_sw passwords (DB2)	113
Verifying the connection to the Process Engine database	113
Completing Oracle post-installation steps	114
Re-enabling Oracle password complexity verification	114
Completing post-installation steps on UNIX platforms	114
Restoring any custom modifications for root and fnsw users (UNIX)	114
Cleaning up before starting Process Engine (UNIX)	115
Editing the /etc/inittab file (UNIX)	115
Modifying the network configuration (UNIX)	116
Completing post-installation steps on Windows platforms	116
Modifying the network configuration (Windows 2008)	116
Modifying the integrity level for executables (Windows 2008)	116
Installing the latest Content Engine client files on Process Engine servers	116
Installing the latest Content Engine client files on Process Engine servers interactively	117
Installing the latest Content Engine client files on Process Engine servers silently	118
Configuring Process Task Manager	119
Verifying connection to the Process Engine database	121
Completing post-installation Process Engine configuration (Windows only)	121
Installing Process Engine software updates	122

Installing and configuring Application Engine 123

Installing Application Engine	123
Installing Application Engine interactively.	124
Installing Application Engine silently	125
Installing Application Engine software updates	126
Installing the latest Content Engine Client files on Application Engine servers	126
Installing the latest Content Engine Client files on Application Engine servers interactively	127

Installing the latest Content Engine Client files on Application Engine servers silently	128
Installing the latest Process Engine Client files on Application Engine servers	129
Installing the latest Process Engine Client files interactively	129
Installing the latest Process Engine Client files silently	130
Configuring Application Engine on the application server	131
Configuring Application Engine on WebSphere Application Server	132
Editing web.xml for container-managed authentication	132
Editing web.xml for SSO	135
Configuring Java Virtual Machine settings for JAAS login and memory	139
Configuring Lightweight Third Party Authentication (LTPA)	140
Configuring stand-alone Lightweight Directory Access Protocol (LDAP)	142
Configuring Lightweight Directory Access Protocol (LDAP) for federated repositories	143
Configuring Application Engine on WebLogic Server	144
Editing web.xml for SSO (optional)	145
Configuring the application server files	146
Enabling communication between Content Engine and Application Engine (WebLogic Server)	148
Enabling passing user credentials to client applications (WebLogic Server 9.2 only)	149
Configuring Application Engine on JBoss Application Server	150
Deploying Application Engine on the application server	152
Deploying Application Engine on WebSphere Application Server	152
Re-creating the WAR or EAR file	153
Deploying the application (WebSphere Application Server 6.1)	154
Deploying the application (WebSphere Application Server 7.0)	155
Deploying Application Engine on WebLogic Server	156
Re-creating the WAR or EAR file	156
Deploying Application Engine	157
Deploying Application Engine on JBoss Application Server	158
Recreating the WAR or EAR file	158
Deploying and starting Application Engine	159
Setting Application Engine bootstrap preferences	159
Setting the bootstrap properties on first login	160
Verifying that a single index has been added for Application Name on the site preferences object store	162
Enabling user access to the workflow subscription wizard	163
Enhanced Timezone Detection	163

Configuration and startup tasks . . . 165

Creating a Process Engine isolated region	165
Creating a Process Engine Connection Point	166
Configuring the Process Engine connection point for Application Engine	167
Setting up Content Engine and client transport SSL security	168
Enabling SSL for Content Engine	169
Enabling SSL between Enterprise Manager and the directory service	171
Setting up Application Engine SSL security	171
Setting up full SSL support on a single Application Engine	172
Setting up SSL redirect on a single Application Engine server	172
Setting up SSL redirect on two Application Engine servers	173
Using Java Applets in an SSL Environment	174
Performing additional configuration tasks	174

Optional installation tasks 177

Installing and Configuring IBM FileNet P8 publishing components	178
Enabling the Process Engine Component Integrator	178
Configuring and starting the Component Manager (on an Application Engine server)	179
Specifying connection between Process Engine and Component Manager (on a Process Engine server)	180
Installing an additional instance of Enterprise Manager	180
Creating additional file storage areas	181
Verifying the file storage area	182
Installing IBM FileNet Deployment Manager	182
Installing Application Integration	184
Installing Application Integration interactively	184
Installing Application Integration silently	185
Verifying your Workplace Application Integration installation	186
Installing Workplace File Tracker	186
Installing the File Tracker software interactively	187
Installing the File Tracker software silently	188
Deploying multiple Application Engine instances	189
Deploying a second instance of Workplace	189
Deploying each additional Workplace instance as an EAR file	190
Enabling Application Engine to use ISRA	191
ISRA SSL support	192
Installing and deploying the Application Engine ISRA servlet	192
Configuring Workplace site preferences for ISRA	194
Logging in to Image Services by using an LDAP account	194
Accessing Image Services library documents	195
Installing and configuring IBM System Dashboard for Enterprise Content Management	195
Modifying an Autonomy K2 server configuration	195
Adding additional K2 administration servers	195
Installing additional Autonomy K2 administration servers (UNIX)	196

Installing additional Autonomy K2 administration servers interactively (UNIX)	197
Installing additional Autonomy K2 administration servers silently (UNIX)	198
Setting environment variables for Content Search Engine (UNIX)	198
Starting or stopping the Autonomy K2 services (UNIX)	199
Installing additional Autonomy K2 administration servers (Windows)	200
Installing additional Autonomy K2 administration servers interactively (Windows)	200
Installing additional Autonomy K2 administration servers silently (Windows)	201
Configuring additional K2 administration servers	201
Moving Autonomy K2 servers to new hardware	202
Moving K2 administration server software to new hardware	202
Removing K2 administration servers from your Content Search Engine configuration	203
Installing the COM compatibility layer (CCL)	203

Part 2. Upgrading and configuring IBM FileNet P8 Platform. 205

Upgrading IBM FileNet P8 documentation 207

Refreshing or updating IBM FileNet P8 documentation	209
Refreshing IBM FileNet P8 documentation without uninstalling	209
Updating IBM FileNet P8 documentation by uninstalling and reinstalling	210
Updating the IBM FileNet P8 documentation on IBM WebSphere Application Server	210
Updating the IBM FileNet P8 documentation on Oracle WebLogic Server	211
Updating the IBM FileNet P8 documentation on JBoss Application Server	212
Updating the documentation search index.	213
Starting and verifying the IBM FileNet P8 documentation web application	214

Upgrading and configuring Content Engine and Content Search Engine . . 217

Upgrading from version 3.5.2	217
Completing pre-upgrade Content Engine configuration	218
Verifying that all in-progress event actions have finished	219
Verifying that publishing requests have been completed	220
Deleting custom subclasses of the PublishRequest object	221

Verifying that all in-progress Content Engine transactions involving content files have finished	221
Granting directory permissions on file stores (Windows only)	222
Renaming storage policies	222
Removing accented characters from file store paths	222
Determining the CBR-enabled properties in an object store	223
Preventing name conflicts with reserved words	223
Upgrading IBM InfoSphere Enterprise Records object stores	223
Running the Content Consistency Checker	224
Moving IBM TotalStorage DR550 fixed content device data	224
Backing up the database.	224
Stopping and disabling all services related to Content Engine.	224
Upgrading Content Engine and related client software	224
Installing or upgrading Content Engine	225
Installing Content Engine interactively	226
Installing Content Engine silently.	227
Installing Content Engine software updates	228
Installing the latest Content Search Engine Client files on Content Engine servers	228
Installing Content Search Engine Client files interactively	229
Installing Content Search Engine Client files silently	230
Installing the latest Process Engine client files on Content Engine servers	231
Upgrading the latest Process Engine client files on Content Engine servers interactively	231
Upgrading the latest Process Engine client files on Content Engine servers silently.	232
Configuring Content Engine	233
Configuring Content Engine instances by using the graphical user interface.	234
Starting Configuration Manager	235
Changing the password save preference	236
Creating a new configuration profile	237
Configuring the Global Configuration Data JDBC data source settings	238
Configuring the login modules (WebSphere and JBoss only)	239
Configuring the directory service provider (LDAP) settings	240
Configuring the bootstrap settings	241
Configuring instances by using the command line.	242
Generating the configuration XML files for a Content Engine instance	243
Editing the configuration XML files for a Content Engine instance.	250
Running the configuration XML files	252
Checking the completion status of Content Engine configuration tasks	257

Deploying upgraded Content Engine instances	259		Creating the initial object store data sources	
Deploying upgraded instances by using the graphical user interface	259		by using the graphical user interface	283
Deploying upgraded instances by using the command line	261		Creating additional object store data sources	
Installing storage device source files	262		by using the graphical user interface	283
Installing Tivoli Storage Manager client and adding native API library paths (WebSphere)	262		Creating the data sources by using the command line	285
Installing Tivoli Storage Manager client	263		Upgrading Content Search Engine software	
Copying the Tivoli Storage Manager API library files to additional servers	263		from version 3.5.2	286
Creating a shared library definition for Tivoli Storage Manager native API library files	263		Production environment upgrades	287
Installing Tivoli Storage Manager client and adding native API library paths (WebLogic)	264		Content Search Engine software upgrade	287
Installing Tivoli Storage Manager client	264		Upgrading Content Search Engine (UNIX)	288
Copying the Tivoli Storage Manager API library files to additional servers	264		Upgrading Content Search Engine	
Creating a shared library definition for Tivoli Storage Manager native API library files	264		interactively (UNIX)	289
Installing Tivoli Storage Manager client and adding native API library paths (JBoss)	267		Upgrading Content Search Engine silently (UNIX)	290
Installing Tivoli Storage Manager client	267		Setting environment variables for Content Search Engine (UNIX)	291
Copying the Tivoli Storage Manager API libraries to additional servers	267		Starting or stopping the autonomy K2 services on UNIX	291
Creating a shared library definition for Tivoli Storage Manager native API library files	267		Upgrading Content Search Engine (Windows)	292
Installing or updating EMC Centera SDK library files	269		Upgrading Content Search Engine	
Installing EMC Centera SDK version 3.2 library files	269		interactively (Windows)	293
Configuring EMC Centera SDK environment variables for version 3.2	270		Upgrading Content Search Engine silently (Windows)	294
Completing Content Engine post-deployment steps	272		Updating the style file of user fields	294
Completing post-deployment steps (WebSphere Application Server)	273		Configuring Content Search Engine	294
Completing post-deployment steps (Oracle WebLogic Server)	273		Configuring services on administration servers	299
Completing post-deployment steps (JBoss Application Server and Active Directory)	273		Configuring Autonomy K2 for version 4.5.1 index areas	299
Verifying the Content Engine deployment	274		Collections directory requirements for Content Search Engine	300
Installing the latest Content Engine client files on other IBM FileNet P8 servers (for staged upgrades)	276		Windows-specific options	301
Establishing the FileNet P8 domain and Global Configuration Data	276		Completing the upgrade	302
Creating the FileNet P8 domain	276		Updating the CFS-IS settings	302
Configuring directory service authentication	277		Upgrading Content Engine data	303
Configuring permissions for a FileNet P8 domain	278		Upgrading Content Engine data using Content Engine Web Upgrade Tool	305
Verifying the trace log file location	278		Deploying Content Engine Web Upgrade Tool	306
Configuring storage devices for upgrades	279		Backing up the version 4.5.1 GCD database	309
Configuring storage devices for migration to UNIX	279		Starting Content Engine Web Upgrade Tool	309
Preparing NetApp SnapLock volumes for upgrade	280		Upgrading a version 3.5.2 FileNet P8 domain into a new version 4.5.1 FileNet P8 domain	310
Creating the data sources for an object store	282		Upgrading a version 3.5.2 FileNet P8 domain into an existing version 4.5.1 FileNet P8 domain	313
			Upgrading Content Engine data using Content Engine Upgrader tool	317
			Preparing the Content Engine Upgrader tool	318
			Backing up the version 4.5.1 GCD database	319
			Running the Content Engine Upgrader tool by using the graphical user interface	319
			Running the Content Engine Upgrader tool by using the command-line interface	325
			Updating the database storage area parameters	328

Completing Content Search Engine upgrade from 3.5.2	328	Configuring upgraded instances by using the graphical user interface	350
Upgrading Enterprise Manager	331	Starting the Configuration Manager graphical user interface	351
Upgrading from version 4.0.1 or 4.5.0	332	Changing the password save preference	351
Completing pre-upgrade Content Engine configuration	334	Creating an upgrade configuration profile	352
Verifying that publishing requests have been completed	334	Configuring the upgraded Content Engine instance	353
Updating the Vital Product Data (VPD) script (version 4.0.1 and Solaris only)	335	Configuring upgraded instances by using the command line	354
Creating the webSphereDefaultIsolationLevel custom property (WebSphere)	335	Installing the latest Process Engine client files on Content Engine servers	356
Verifying permissions on the Engine-DS.xml file (JBoss only)	336	Upgrading the latest Process Engine client files on Content Engine servers interactively	356
Backing up the database	336	Upgrading the latest Process Engine client files on Content Engine servers silently	357
Shutting down CFS Exporter	337	Deploying upgraded Content Engine instances	358
Preventing name conflicts with reserved words	337	Deploying upgraded instances by using the graphical user interface	359
Removing the deployed FileNetEngine application	337	Deploying upgraded instances by using the command line	360
Clearing the web application server cache	338	Installing storage device source files	362
Editing XA data source XML files (Oracle and JBoss 4)	339	Installing Tivoli Storage Manager client and adding native API library paths (WebSphere)	362
Uninstalling Content Engine and Content Search Engine Client Updater (Version 4.0.1 and AIX)	339	Installing Tivoli Storage Manager client	362
Uninstalling Content Engine interactively (version 4.0.1 and AIX)	340	Copying the Tivoli Storage Manager API libraries to additional servers	363
Uninstalling Content Engine silently (AIX)	340	Creating a shared library definition for Tivoli Storage Manager native API library files	363
Uninstalling Content Search Engine Client Updater interactively (version 4.0.1 and AIX)	341	Installing Tivoli Storage Manager client and adding native API library paths (WebLogic)	363
Uninstalling Content Search Engine Client Updater silently (version 4.0.1 and AIX)	341	Installing Tivoli Storage Manager client	363
Upgrading Content Engine software from version 4.0.1 or 4.5.0	341	Copying the Tivoli Storage Manager API library files to additional servers	364
Upgrading Content Engine software interactively (Windows)	342	Creating a shared library definition for Tivoli Storage Manager native API library files	364
Upgrading Content Engine software interactively (UNIX)	342	Installing Tivoli Storage Manager client and adding native API library paths (JBoss)	366
Upgrading Content Engine software silently (Windows)	343	Installing Tivoli Storage Manager client	366
Upgrading Content Engine software silently (UNIX)	344	Copying the Tivoli Storage Manager API libraries to additional servers	367
Upgrading Enterprise Manager	344	Creating a shared library definition for Tivoli Storage Manager native API library files	367
Installing Content Engine software updates	345	Installing or updating EMC Centera SDK library files	368
Installing the latest Content Search Engine Client files on Content Engine servers	345	Installing EMC Centera SDK version 3.2 library files	369
Removing the existing Content Search Engine Client 4.0.1 files from Content Engine Server machines	346	Configuring EMC Centera SDK environment variables for version 3.2	370
Collecting current Content Engine deployment data	346	Completing Content Engine post-deployment steps	372
Installing Content Engine Search Client files	347	Completing post-deployment steps (WebSphere Application Server)	373
Installing Content Search Engine Client files interactively	347	Completing post-deployment steps (Oracle WebLogic Server)	373
Installing Content Search Engine Client files silently	348	Completing post-deployment steps (JBoss Application Server and Active Directory)	373
Granting directory permissions to the Configuration Manager user	349	Verifying the Content Engine deployment	374
Configuring Content Engine instances upgraded from version 4.0.1 or 4.5.0	350		

Checking the automatic upgrade status for Content Engine data	375	Setting the f_maint and f_sw passwords (DB2)	406
Installing the latest Content Engine client files on other IBM FileNet P8 servers (for staged upgrades)	376	Setting the f_maint and f_sw passwords (Oracle and Microsoft SQL Server)	406
Upgrading Content Search Engine software from version 4.0.1 or 4.5.0	377	Restoring any custom modifications for root and fnsw users (UNIX)	407
Production environment upgrades	377	Editing the /etc/inittab file.	407
Upgrading Content Search Engine	378	Upgrading Process Engine silently	408
Upgrading Content Search Engine software (UNIX)	378	Verifying the Process Engine database connection	408
Upgrading Content Search Engine software (Windows)	384	Verifying the Process Engine database connection (Microsoft SQL Server)	409
Setting the logon user for the K2 Administration Server service (Windows)	388	Verifying the Process Engine database connection (DB2)	409
Updating the style file of user fields.	389	Verifying the Process Engine database connection (Oracle)	410
Upgrading and configuring Process Engine	391	Upgrading Process Engine silently	411
Completing pre-upgrade Process Engine configuration	391	Upgrading the Process Engine software silently (Windows).	411
Completing pre-upgrade steps for upgrades from Process Engine Version 3.5	392	Upgrading the Process Engine software silently (UNIX)	412
Updating all isolated regions	393	Encrypting passwords for Process Engine	413
Completing pre-upgrade steps for Process Analyzer installations	393	Setting the f_maint and f_sw passwords (DB2)	414
Verifying that all Process Analyzer 3.5 events have been published	393	Setting the f_maint and f_sw passwords (Oracle and Microsoft SQL Server)	414
Verifying that all Process Engine 3.5 events have been transmitted to Process Analyzer	394	Restoring any custom modifications for root and fnsw users (UNIX)	415
Purging event logs and statistics records	395	Editing the /etc/inittab file.	415
Stopping all Process Engine-related services and applications (Windows)	396	Upgrading the Content Engine client files on Process Engine servers	416
Stopping all Process Engine-related services and applications (UNIX).	397	Uninstalling Content Engine client 4.0.x instances	416
Completing pre-upgrade steps for upgrades from Process Engine 4.0 or 4.5.	397	Uninstalling Content Engine Client 4.0.x instances on Windows	416
Updating all isolated regions	398	Uninstalling Content Engine Client 4.0 instances on UNIX	417
Purging event logs and statistics records	399	Upgrading the Content Engine client files	417
Stopping all Process Engine-related services and applications (Windows)	399	Upgrading the latest Content Engine client files on Process Engine servers interactively	418
Stopping all Process Engine-related services and applications (Unix)	400	Upgrading the latest Content Engine client files on Process Engine servers silently	419
Upgrading Process Engine	400	Completing post-upgrade Process Engine configuration	421
Upgrading Process Engine interactively	401	Completing the upgrade from Process Engine 3.5	421
Verifying the Process Engine database connection	401	Completing the upgrade from Process Engine 3.5 by database type	422
Verifying the Process Engine database connection (Microsoft SQL Server)	402	Completing the upgrade from Process Engine 3.5 (Oracle)	422
Verifying the Process Engine database connection (DB2)	402	Completing the upgrade from Process Engine 3.5 (DB2)	423
Verifying the Process Engine database connection (Oracle)	403	Completing the upgrade from Process Engine 3.5 (SQL Server)	425
Upgrading Process Engine interactively	404	Removing existing routers in Process Task Manager	427
Upgrading the Process Engine software interactively (Windows)	404	Updating the Process Engine security	427
Upgrading the Process Engine software interactively (UNIX)	405	Running post-upgrade scripts Microsoft SQL Server and DB2.	429
Setting the f_maint and f_sw passwords	406		

Running post-upgrade scripts (Microsoft SQL Server)	430
Running post-upgrade scripts (DB2).	431
Configuring contiguous free memory for Process Engine (Windows)	431
Migrating routers and updating isolated regions	432
Configuring new regions in IBM FileNet Enterprise Manager	432
Configuring new regions in Process Task Manager	433
Updating email notification.	433
Backing up the database and restarting software	434
Completing the upgrade from Process Engine 4.0, 4.5.0, or higher	434
Configuring contiguous free memory for Process Engine (Windows)	436
Backing up the database and restarting software	436
Installing Process Engine software updates	437
Installing the latest Process Engine client files on other IBM FileNet P8 servers (for staged upgrades).	437

Upgrading and configuring

Application Engine	439
Preparing for Application Engine upgrade.	440
Upgrading Application Engine	443
Upgrading Application Engine from 3.5	443
Upgrading Application Engine interactively	444
Upgrading Application Engine silently	445
Upgrading Application Engine from 4.0	446
Upgrading Application Engine from 4.0 interactively	446
Upgrading Application Engine from 4.0 silently	447
Installing Application Engine software updates	448
Installing the latest Content Engine client files on Application Engine servers	449
Removing the Content Engine 4.0 Client files from Application Engine servers	449
Removing Content Engine 4.0 Client files from Application Engine servers (UNIX)	450
Removing Content Engine 4.0 Client files from Application Engine servers (Windows)	450
Installing the latest Content Engine Client files on Application Engine servers interactively	451
Installing the Content Engine Client files silently	452
Installing the latest Process Engine client files on Application Engine servers	454
Upgrading the latest Process Engine Client files interactively	455
Upgrading the latest Process Engine Client files silently	456
Configuring Application Engine upgrades from 3.5	457
Configuring Application Engine upgrades from 3.5 on WebSphere Application Server	458
Editing web.xml for container-managed authentication	458
Editing web.xml for SSO	461

Configuring Java Virtual Machine settings for JAAS login and memory	465
Configuring Lightweight Third Party Authentication (LTPA)	466
Configuring stand-alone Lightweight Directory Access Protocol (LDAP)	468
Configuring Lightweight Directory Access Protocol (LDAP) for federated repositories	469
Configuring Application Engine upgrades from 3.5 on WebLogic Server	470
Editing web.xml for SSO (optional)	470
Configuring the application server files.	472
Enabling communication between Content Engine and Application Engine (WebLogic Server)	474
Enabling passing user credentials to client applications (WebLogic Server 9.2 only)	475
Configuring Application Engine upgrades from 3.5 on JBoss Application Server	475
Manually copying custom data	478
Deploying upgraded instances of Application Engine	478
Deploying upgraded instances of Application Engine on WebSphere Application Server	479
Re-creating the WAR or EAR file	479
Deploying Application Engine.	480
Deploying the application (WebSphere Application Server 6.1)	480
Deploying the application (WebSphere Application Server 7.0)	481
Deploying Application Engine on WebLogic Server	482
Re-creating the WAR or EAR file	483
Deploying Application Engine.	483
Deploying Application Engine on JBoss Application Server	484
Re-creating the WAR or EAR file	484
Deploying and starting Application Engine	485
Completing post-upgrade Application Engine configuration	486

Upgrading add-on components. 487

Upgrading Application Integration and File Tracker	487
Upgrading Workplace Application Integration	488
Verify your Workplace Application integration upgrade	489
Upgrading Workplace File Tracker	489
Upgrading IBM FileNet publishing components	489
Upgrading server-side scripts and COM objects	489
File document handler	490
Log event handler	491
Send eMail handler	493
Upgrading Image Services Resource Adapter servlet.	494
ISRA SSL support	495
Upgrading the Application Engine Image Services Resource Adapter servlet	496
Configuring the Workplace site preferences for ISRA support	498
Setting the ISRA interface servlet URL	498
Logging on to Image Services through LDAP	498

Accessing IS library documents	499
Installing component software updates	499

Part 3. Removing software 501

Removing the IBM FileNet P8 documentation 503

Removing the FileNet P8 documentation from a WebSphere Application Server.	503
Removing the FileNet P8 documentation from a WebLogic Server	504
Removing the FileNet P8 documentation from a JBoss Application Server.	504

Removing Content Engine 505

Removing part or all of a Content Engine installation interactively by using the Windows control panel	505
Removing an entire Content Engine installation interactively (UNIX)	505
Removing Content Engine silently	506
Removing data associated with Content Engine	506

Removing Content Search Engine . . . 507

Removing additional locales (UNIX) 509

Removing additional locales (Windows). 511

Removing Process Engine (Windows) 513

Removing Process Engine (UNIX) . . . 515

Removing Application Engine (WebSphere). 517

Removing Application Engine (WebLogic) 519

Removing Application Engine (JBoss Application Server) 521

Removing the Application Engine ISRA servlet 523

Removing Workplace Application Integration 525

Removing or modifying Workplace Application Integration interactively	525
Removing Workplace Application Integration silently	525

Removing Workplace File Tracker . . . 527

Removing Workplace File Tracker interactively	527
Removing Workplace File Tracker silently	527

Part 4. Appendixes 529

Appendix A. Configuration Manager reference 531

Overview of Configuration Manager	532
Configuration profile concepts.	532
Using the graphical and command-line user interfaces.	534
Gathering Configuration Manager values by using the installation and upgrade worksheet	534
Handling passwords in Configuration Manager	535
Accessing the Configuration Manager log files	535
Adding an SSL signer to the Configuration Manager keystore (WebSphere)	536
Correcting an SSL Signer Exchange Prompt error (WebSphere).	537
Configuration Manager user interface reference	538
Starting Configuration Manager	538
Configuration Manager window	539
Main toolbar	540
Profile toolbar	540
Task toolbar	541
Console toolbar.	541
Configuration Manager menus and commands	542
Working with Configuration Manager	545
Configuring a Content Engine instance.	546
Setting the password save preference	546
Creating a profile for a new installation	546
Creating a profile for an upgrade.	547
Opening and closing an existing profile or task	547
Editing the application server properties	548
Editing the properties for a specific task	548
Editing the configure JDBC data source task	549
Editing the configure LDAP task	549
Editing the configure bootstrap properties settings	550
Editing the deploy application task	550
Applying the property settings by running a specific task	550
Applying the JDBC data source settings	551
Configuring the login modules	551
Applying the LDAP settings	552
Applying the bootstrap properties settings	552
Deploying the application	552
Adding an additional task to your profile	552
Deleting a task from a profile	553
Running all tasks at the same time	553
Running a single task	554
Checking the task status.	554
Viewing the session log	555
Saving your changes to a task or profile	555
configmgr.ini parameters	555
Configuration Manager command-line reference	555
Running Configuration Manager commands	555
How to read the syntax diagrams	557
checkstatus command	557
execute command	561
generateconfig command	566

generateupgrade command (with Servers.xml file)	572
generateupgrade command (without Servers.xml file)	573
gui command	575
listservers command	575
listtasks command	575
movetask command	579
removetask command	582
storepasswords command	585

Appendix B. Troubleshooting installation and upgrade. 589

AddOn installation can fail with resource unavailable exception.	589
Application server does not start after installation and shutdown	590

Cannot save Process Task Manager security settings	591
Verifying the Content Engine server is available to Process Engine on the network	592
Verifying that the Process Engine can connect to a FileNet Engine Web page on Content Engine	592
Verifying that Process Engine can connect to Content Engine by using the Content Engine URI	593

Notices 595

Trademarks	597
----------------------	-----

Index 599

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/v4r5m1/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=3278&uid=swg27010422

“How to send your comments”

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

“Contacting IBM” on page xiv

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 and configuring IBM FileNet P8 Platform

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

As an alternative to the Application Engine component and its Workplace user application, you can set up Workplace XT. See the Workplace XT documentation for details.

“Installing IBM FileNet P8 Platform documentation” on page 3

You can link to the online version of the IBM FileNet P8 Platform documentation, or install and deploy the documentation package as part of your FileNet P8 environment.

“Installing and configuring Content Engine” on page 11

Content Engine is the content-management component of IBM FileNet P8 platform. To set up Content Engine, you install the content-management server software on an application server, and then configure and deploy the Content Engine web application. You must also configure the Global Configuration Data (GCD), create the FileNet P8 domain, and create at least one object store. The GCD contains system information about your particular configuration. The object stores contain information about the documents, records, forms, and other business objects that you store in your IBM FileNet P8 system.

“Installing and configuring Content Search Engine” on page 79

This topic explains how to install and configure Content Search Engine.

“Installing and configuring Process Engine” on page 103

Installing and configuring Process Engine is a process requiring multiple steps, and the steps must be followed in sequence.

“Installing and configuring Application Engine” on page 123

Application Engine provides a client application called Workplace that you can use to access the information managed by Content 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 165

After you install the IBM FileNet P8 components, there are some additional steps to configure the IBM FileNet P8 system. After you configure the IBM FileNet P8 components, familiarize yourself with IBM FileNet P8 system startup and shutdown procedures. See the **System Administration** → **Enterprise-wide Administration** → **Startup and Shutdown** help topic.

“Optional installation tasks” on page 177

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

Installing IBM FileNet P8 Platform documentation

You can link to the online version of the IBM FileNet P8 Platform documentation, or install and deploy the documentation package as part of your FileNet P8 environment.

You can link your FileNet P8 software directly to the IBM FileNet P8 Platform Version 4.5.1 information center on www.ibm.com. The advantages of linking to the [ibm.com](http://www.ibm.com) information center are as follows:

- You do not have to maintain a documentation server or information center.
- The documentation is always up to date.

If you want to use the online information center, you do not need to install any documentation in your environment. During the installation and configuration of your IBM FileNet P8 Platform components, provide the following link for your P8 documentation URL: <http://publib.boulder.ibm.com/infocenter/p8docs/v4r5m1/topic/com.ibm.p8.doc>

If you want the documentation to be deployed directly in your FileNet P8 environment, you must install the `ecm_help` documentation package.

The procedures you follow to install the IBM FileNet P8 documentation package depend on whether your installation needs to include more than the core documentation for IBM FileNet P8 Platform. If you need to add IBM FileNet P8 documentation, then you must complete additional steps.

The other documentation that you might need to install can be for IBM FileNet P8 expansion products, for example, IBM FileNet Process Analyzer, IBM FileNet Process Simulator, IBM FileNet eForms for P8, IBM FileNet Content Federation Services, or IBM InfoSphere™ Enterprise Records. You might also include auxiliary documentation that includes release notes, technical notices, or documentation that is provided with a customized application.

1. “Before you install the `ecm_help` documentation package” on page 4
If you intend to access online help from any IBM FileNet P8 applications, for example, Workplace, Enterprise Manager, and Process Task Manager, or use the full-text search feature, you must install the documentation for IBM FileNet P8 Platform information center on a supported Web application server, for example, IBM WebSphere® Application Server, Oracle WebLogic Server, or JBoss Application Server.
2. “Installing the core IBM FileNet P8 Platform documentation” on page 4
You must install the core IBM FileNet P8 Platform documentation as a Web application on a supported application server to view and search installation, administration, and user information.
3. “Installing and re-indexing expansion-products, custom, and auxiliary documentation” on page 6
To install documentation for IBM FileNet P8 expansion products, you must copy that documentation onto the application server where IBM FileNet P8 Platform documentation is already installed. You then rebuild the documentation search index.
4. “Starting and verifying the IBM FileNet P8 documentation Web application” on page 9
After you install and optionally index the IBM FileNet P8 documentation again

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

5. "Backing up and redeploying the FileNet P8 documentation" on page 9
After you verify the installation of your FileNet P8 documentation, it is a best practice to store a backup copy. This action prepares you for quicker recovery from disaster and for future redeployment to other servers. Backing up a copy is especially advisable if you have expansion-product documentation installed with the core IBM FileNet P8 Platform documentation.

Before you install the ecm_help documentation package

If you intend to access online help from any IBM FileNet P8 applications, for example, Workplace, Enterprise Manager, and Process Task Manager, or use the full-text search feature, you must install the documentation for IBM FileNet P8 Platform information center on a supported Web application server, for example, IBM WebSphere Application Server, Oracle WebLogic Server, or JBoss Application Server.

Optionally, you can install and index auxiliary documentation that is available only on the IBM Web site. You make this documentation searchable with the rest of the installed product documentation. For a complete list of additional documentation, see "Gather auxiliary documentation" in *Plan and Prepare Your Environment for IBM FileNet P8*.

You can use multipart root directories if your application server supports them, for example, /docs/ecm_help instead of simply /ecm_help.

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

Consider the following installation requirements by application server type:

Table 1. Documentation installation requirements

Application server	Requirement
WebSphere Application Server	IBM FileNet P8 documentation must be installed as a WAR file (ecm_help.war).
WebLogic Server	You cannot install the IBM FileNet P8 help files as WAR or EAR files because the internal documentation search engine cannot function as expected. You must extract the ecm_help.war file or use the ecm_help flat file structure to install the IBM FileNet P8 documentation.
JBoss Application Server	You cannot install the IBM FileNet P8 information center files as WAR or EAR files because the internal documentation search engine cannot function as expected. You must extract the ecm_help.war file or use the ecm_help flat file structure to install the IBM FileNet P8 documentation.

Installing the core IBM FileNet P8 Platform documentation

You must install the core IBM FileNet P8 Platform documentation as a Web application on a supported application server to view and search installation, administration, and user information.

Before you install the FileNet P8 information center, you must ensure that you have Java™ support enabled on the application server you choose. You must also fulfill other application server requirements and determine the scope of the documentation you plan to install.

- For Oracle WebLogic Server and JBoss Application Server, a valid Java SDK must be available for the application server.
- To ensure that the documentation can be searched, ensure that JavaScript™ support is enabled on each browser client.
- Depending on your operating system and application server levels, your options might be slightly different from the options that are documented.
- For JBoss Application Server, set the value of the following two attributes in the \jboss-4.0.5.GA\server\default\deploy\jbossweb-tomcat55.sar\META-INF\jboss-service.xml file to true, where each <attribute> element appears on a single line, for example:

```
<attribute name=
"Java2ClassLoadingCompliance">true</attribute>

<attribute name=
"UseJBossWebLoader">true</attribute>
```

To install the core IBM FileNet P8 Platform documentation:

1. Access the IBM FileNet P8 Platform documentation package and perform the following actions. The deploy operation can take several minutes because of the size of the documentation files.

Option	Description
WebSphere Application Server	<ol style="list-style-type: none"> 1. Copy the IBM FileNet P8 ecm_help.war file from the IBM FileNet P8 documentation package to the local hard drive. 2. From the WebSphere administrative console, install the ecm_help.war file as a Web application by using ecm_help 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.
Oracle WebLogic Server	<ol style="list-style-type: none"> 1. Extract the IBM FileNet P8 ecm_help.war file or copy the entire ecm_help directory structure from the IBM FileNet P8 documentation package to a location on the local hard drive. 2. From the WebLogic administrative console, install a new Web application for the IBM FileNet P8 Platform documentation.

Option	Description
JBoss Application Server	From the IBM FileNet P8 documentation package, perform one of the following actions to create a deployable <code>ecm_help.war</code> directory on the JBoss application server: <ul style="list-style-type: none"> • Extract the <code>ecm_help.war</code> file to the <code>ecm_help.war</code> directory. • Copy the <code>ecm_help</code> directory to the JBoss application server and rename it to <code>ecm_help.war</code>.

2. Add more documentation or continue with verifying the documentation Web application:
 - To add documentation for any IBM FileNet P8 expansion product or any auxiliary documentation, such as release notes or technical notices, continue with “Installing and re-indexing expansion-products, custom, and auxiliary documentation.”
 - If you have no further documentation to install, continue with “Starting and verifying the IBM FileNet P8 documentation Web application” on page 9.

Installing and re-indexing expansion-products, custom, and auxiliary documentation

To install documentation for IBM FileNet P8 expansion products, you must copy that documentation onto the application server where IBM FileNet P8 Platform documentation is already installed. You then rebuild the documentation search index.

Optionally, you can copy auxiliary documentation that is available solely on the IBM Web site into your IBM FileNet P8 documentation Web application. You can then search the auxiliary documentation in the documentation search feature. For example, you can copy *IBM FileNet P8 Release Notes*[®] and *IBM FileNet P8 Troubleshooting Guide* from the IBM Web site to the documentation server. Users looking for product news or troubleshooting information can then find information quickly from the documentation Web application.

Also, you might be required to install documentation for a customized application onto the IBM FileNet P8 documentation server. Check with your application vendor for installation details.

Important: Every time you update the documentation search index, a backup copy of the files in the existing `Index/core` subdirectory is automatically copied to the `Index/Index01d` subdirectory. If you must return to the previous indexed state, you can reapply these backed up files to the `Index/core` subdirectory. You must first move or delete the files that are created there.

To install and index expansion product, custom, and auxiliary documentation:

1. Determine the expansion products documentation location, either on local media source or a network location. For most expansion products, use the documentation package that is included as part of the particular software product.
2. Stop the IBM FileNet P8 Platform `ecm_help` documentation application:

Option	Description
IBM WebSphere Application Server	Use the administrative console.
Oracle WebLogic Server	Use the administrative console.
JBoss Application Server	Shut down JBoss.

3. Verify that no processes are accessing the documentation Web application.
4. Copy the IBM FileNet P8 expansion product documentation, to the core IBM FileNet P8 Platform documentation location. Include all directories and files below the `ecm_help` directory.
By default, the IBM FileNet P8 Platform documentation is installed in an `ecm_help` directory.
You can copy documentation sets for more than one expansion product to the documentation application server. When you finish, you have one `ecm_help` directory structure that contains the core documentation set and one or more sets of expansion product documentation files.
5. Download the latest Web-posted updates of planning and installation guides for IBM FileNet P8 Platform and the various expansion products you use.
6. Download any auxiliary documentation you want included in documentation searches to the `ecm_help/installation/web` directory in the core IBM FileNet P8 Platform documentation location.
7. Install the documentation for any custom application that is integrated with the IBM FileNet P8 Platform documentation. See the instructions provided with that software product.
8. To index the new documentation, open a terminal or command prompt on the application server.
9. From the command line, navigate to the search subdirectory under the application root directory, for example, `ecm_help`.
10. Complete the search indexing steps:

Option	Description
<p>UNIX®</p>	<ol style="list-style-type: none"> 1. Apply chmod 755 permissions on the indexFiles.sh file, which is set to read-only permissions in the documentation package. 2. Using a text editor, open the indexFiles.sh file. 3. If necessary for your environment, set the JAVA_HOME variable in the script file with the path to your Java Runtime Environment (JRE) installation location. Important: The Java JRE installation subdirectory can be user-defined, so substitute your actual location. 4. Save your changes and close the text editor. 5. From the ecm_help/search directory, run the updated indexFiles.sh search-indexing script. As you run the script file, you might notice periodic Parse Abort errors. You can ignore these error conditions because they are benign and do not affect the overall indexing process.
<p>Windows®</p>	<ol style="list-style-type: none"> 1. Modify the search-indexing script file by setting Read and Execute permissions on the indexFiles.bat file, which is preset to read-only permissions in the documentation package. 2. Using a text editor, open the indexFiles.bat search-indexing script file. 3. If necessary for your environment, set the JAVA_HOME variable in the script file with the path to your Java Runtime Environment (JRE) installation location. Important: The Java JRE installation subdirectory can be user-defined, so substitute your actual location. 4. Save your changes and close the text editor. 5. From the ecm_help/search directory, run the updated indexFiles.bat search-indexing script file. As you run the script file, you might notice periodic Parse Abort errors. You can ignore these error conditions because they are benign and do not affect the overall indexing process.

Related information



Product documentation for IBM FileNet P8 Platform

Download the latest web-posted updates of the planning and installation guides, as well as the rest of the IBM FileNet P8 Platform documentation.

Starting and verifying the IBM FileNet P8 documentation Web application

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

To verify the IBM FileNet P8 documentation installation:

1. Start the IBM FileNet P8 documentation Web application (`ecm_help`) on the application server.
2. 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	<code>http://yourdocserver:9080/ecm_help/</code>
Oracle WebLogic Server	<code>http://yourdocserver:7001/ecm_help/</code>
JBoss Application Server	<code>http://yourdocserver:8080/ecm_help/</code>

If the installation was a success, the IBM FileNet P8 documentation opens the same way as for an IBM FileNet P8 component application.

3. Note the URL for your application server because you must enter it as the documentation URL for the IBM FileNet P8 components while running installation programs or setting site preferences later, for example, in Workplace or Workplace XT.
4. Click the **Search** link on the Help Directory toolbar and verify that it opens the documentation Search page.
5. Enter a value for your Search query and verify that the query runs as expected.
6. Select one of the Search query result links and verify that the help page opens.

Backing up and redeploying the FileNet P8 documentation

After you verify the installation of your FileNet P8 documentation, it is a best practice to store a backup copy. This action prepares you for quicker recovery from disaster and for future redeployment to other servers. Backing up a copy is especially advisable if you have expansion-product documentation installed with the core IBM FileNet P8 Platform documentation.

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

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

Installing and configuring Content Engine

Content Engine is the content-management component of IBM FileNet P8 platform. To set up Content Engine, you install the content-management server software on an application server, and then configure and deploy the Content Engine web application. You must also configure the Global Configuration Data (GCD), create the FileNet P8 domain, and create at least one object store. The GCD contains system information about your particular configuration. The object stores contain information about the documents, records, forms, and other business objects that you store in your IBM FileNet P8 system.

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

When you deploy Content Engine in a WebSphere Application Server managed environment, you must install and configure Content Engine on the network deployment node to avoid cross-network configuration issues. Install and configure Content Engine on the administration server. Then use the administration server tools to deploy the Content Engine EAR file to the managed servers. The managed servers can be in a cluster.

When you deploy Content Engine in a WebSphere Application Server non-managed environment, install and configure Content Engine on a single server in the environment. After deploying the bootstrapped Content Engine EAR file on the initial server, copy the bootstrapped EAR file to the other servers. On each additional server, configure the LDAP provider, the JDBC data sources, and the login modules. Then deploy the bootstrapped EAR file that was copied from the initial server.

When you deploy Content Engine in an Oracle WebLogic Server managed environment, you must install and configure Content Engine on the administrative node to avoid cross-network configuration issues. Install and configure Content Engine on the administration server. Then use the administration server tools to deploy the Content Engine EAR file to the managed servers. The managed servers can be in a cluster.

Content Engine has no managed deployment capability. When you deploy Content Engine in a JBoss Application Server non-managed environment, install and configure Content Engine on an initial server in the environment, and then copy the Content Engine EAR file from the initial server to the other servers in the environment.

1. "Installing Content Engine and related client software" on page 12
You must install the Content Engine software and related client software to place the binary files for its components on the server.
2. "Configuring Content Engine" on page 21
You can configure and deploy all of your Content Engine instances with Configuration Manager. Configuration Manager prepares the Content Engine application for deployment on the application server. A single Content Engine application instance equates to one deployed application on your application server.

3. “Deploying Content Engine instances” on page 48
Depending on your environment, you can use the Configuration Manager graphical user interface, or the command line, to deploy Content Engine instances.
4. “Installing storage device source files” on page 55
If your IBM FileNet P8 system includes IBM Tivoli® Storage Manager or EMC Centera devices, you must install files on the Content Engine server.
5. “Completing Content Engine post-deployment steps” on page 65
You must complete the post-deployment web application server configuration before you can put an IBM FileNet P8 system into production.
6. “Verifying the Content Engine deployment” on page 67
You can verify that the Content Engine deployment was successful by accessing the IBM FileNet P8 System Health page.
7. “Establishing the FileNet P8 domain and Global Configuration Data (GCD)” on page 69
With Content Engine installed and deployed, you must use IBM FileNet Enterprise Manager to create a FileNet P8 domain. You can also use Enterprise Manager to set a URL to the FileNet P8 online help if you did not specify the location when you ran the Content Engine installation program.
8. “Creating the data sources for an object store” on page 71
Each object store in your site requires its own JDBC data sources. You can configure the data sources by using the Configuration Manager graphical user interface or the command line.
9. “Creating the initial object store” on page 76
You create an initial object store in Content Engine to store your documents and other objects. After an object store is created, you can refine its definition and add content to it.
10. “Verifying the Content Engine installation” on page 77
You can verify that the Content Engine installation succeeded by using IBM FileNet Enterprise Manager to create a folder and a document in each object store and then check the new document out and in.

Installing Content Engine and related client software

You must install the Content Engine software and related client software to place the binary files for its components on the server.

1. “Installing Content Engine” on page 13
You must install the Content Engine software to place the binary files for its components on the server. You can install the software interactively with a wizard or silently from the command line.
2. “Installing Enterprise Manager” on page 15
You must install IBM FileNet Enterprise Manager to administer content in an Enterprise Content Management system. You install this software by running the Content Engine installer.
3. “Installing Content Engine software updates” on page 16
You must install the latest software updates, fix packs, or interim fixes for the Content Engine software to ensure optimal operation.
4. “Installing the latest Content Search Engine Client files on Content Engine servers” on page 17
The Content Search Engine Client files make it possible for the Content Search Engine server component to communicate with the Content Engine servers.
5. “Installing the latest Process Engine Client files on Content Engine servers” on page 19

Install the Process Engine Client files on the Content Engine to enable communication between Content Engine and Process Engine. You can install the files interactively by using the installation wizard or silently by using the command line and a silent input file.

Installing Content Engine

You must install the Content Engine software to place the binary files for its components 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.

You can install the Content Engine components shown in the following table. Note that some of the components can be installed only on Windows.

Table 2. Content Engine components

Component	Required Platform	Description
Content Engine Server	UNIX or Windows	Install this software as the major Content Engine component. When you install Content Engine Server, Configuration Manager is also installed.
Configuration Manager	UNIX or Windows	Install this software as the primary tool to configure and maintain Content Engine installations. When you install Content Engine Server, Configuration Manager is also installed.
.NET Clients (including Enterprise Manager)	Windows only	Install this software only on machines where you intend to run either the Enterprise Manager administrative client or a customized client application.
Content Engine Upgrader	Windows only	Install this tool only if you are upgrading Content Engine and Content Search Engine data from version 3.5.
FileNet Deployment Manager	Windows only	Install this tool only if you must deploy test systems into full production. See the IBM FileNet P8 help topic Application Deployment → Get Started with FileNet Deployment Manager for details about how you might use this tool.


“Installing Content Engine interactively” on page 14

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

“Installing Content Engine silently”

When you install Content Engine silently, you run a command in the Content 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 Engine interactively

To install Content Engine interactively, you run a wizard that prompts you for an installation path and the Content 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 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 Engine values, filter by **CE Installer** in the **Installation or Configuration Program** column.

2. Log on as *ce_install_user* to the application server machine where you are going to install Content Engine software.
3. Navigate to the Content 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
AIX®	P8CE-4.5.1-AIX.BIN
HPUX	P8CE-4.5.1-HPUX.BIN
HPUXi	P8CE-4.5.1-HPUXI.BIN
Linux®	P8CE-4.5.1-LINUX.BIN
Linux on System z®	P8CE-4.5.1-ZLINUX.BIN
Solaris	P8CE-4.5.1-SOL.BIN
Windows	P8CE-4.5.1-WIN.EXE

5. Complete the Content 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 Engine *ce_install_path/ce_install_log_4_5_1.txt* error log file, where *ce_install_path* is the location where Content Engine is 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 Engine silently

When you install Content Engine silently, you run a command in the Content 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 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 Engine values, filter by **CE Installer** in the **Installation or Configuration Program** column.

2. Log on as `ce_install_user` to the application server machine where you are going to install Content Engine software.
3. Navigate to the Content 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
AIX	P8CE-4.5.1-AIX.BIN -f CE_silent_install.txt -i silent
HPUX	P8CE-4.5.1-HPUX.BIN -f CE_silent_install.txt -i silent
HPUXi	P8CE-4.5.1-HPUXI.BIN -f CE_silent_install.txt -i silent
Linux	P8CE-4.5.1-LINUX.BIN -f CE_silent_install.txt -i silent
Linux on System z	P8CE-4.5.1-ZLINUX.BIN -f CE_silent_install.txt -i silent
Solaris	P8CE-4.5.1-SOL.BIN -f CE_silent_install.txt -i silent
Windows	P8CE-4.5.1-WIN.EXE -f CE_silent_install.txt -i silent

6. When the installation completes, check for errors in the Content Engine error log file `ce_install_path/ce_install_log_4_5_1.txt`, where `ce_install_path` is the location where Content Engine is 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

You must install IBM FileNet Enterprise Manager to administer content in an Enterprise Content Management system. You install this software by running the Content Engine installer.

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 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 Engine server indicates that Enterprise Manager has been installed.

Important: You cannot install Enterprise Manager on a UNIX 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 Engine values, filter by **CE 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 Windows components.

Option	Description
Microsoft® Windows XP, Microsoft Windows Server 2003	Microsoft .NET Framework 2.0 and Web Services Enhancements (WSE) 3.0
Content Engine version 4.5.1 Fix Pack 002 or higher with Microsoft Windows Vista, Microsoft Windows Server 2008, or Microsoft Windows 7	Microsoft .NET Framework 3.0 and Windows Communication Foundation (WCF)

4. Access the Content 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: P8CE-4.5.1-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,AdminTools 3. Save your edits. 4. Run the following command in the software package on a single line: P8CE-4.5.1-WIN.EXE -f CE_silent_install.txt -i silent

Installing Content Engine software updates


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

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

To install the Content Engine software updates:

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

Related information

 [IBM FileNet P8 Platform documentation and support](#)
Obtain the latest Content Engine software updates, as well as the rest of the IBM FileNet P8 Platform documentation.

Installing the latest Content Search Engine Client files on Content Engine servers


The Content Search Engine Client files make it possible for the Content Search Engine server component to communicate with the Content Engine servers.

Important: With the initial release of Content Engine 4.5.1, the Content Search Engine 4.5.1 client files are included. Therefore, you are not required to manually install these client files on a new Content Engine server. However, if fix packs of these client files become available, install them manually before you use Configuration Manager to configure and deploy Content Engine. For instructions on how to obtain the latest Content Search Engine Client software updates, access the IBM FileNet P8 Platform support site.

You can manually install Content Search Engine Client files either interactively or silently:

1. “Installing Content Search Engine Client files interactively”
You can install the Content Search Engine Client files interactively by running the installation program on all application server machines where Content Engine Server is installed.
2. “Installing Content Search Engine Client files silently” on page 18
You can install the Content Search Engine Client files silently by editing a silent input file and running the installation program from a command line. You must install Content Search Engine Client files on all application server machines where Content Engine Server is 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 Content Search Engine Client files interactively

You can install the Content Search Engine Client files interactively by running the installation program on all application server machines where Content Engine Server is installed.

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

To install Content Search Engine Client files:

1. On the machine where Content Engine is to be deployed, log on as `ce_install_user`.
2. Locate the Content Search Engine Client installation software. It must be the same version as your Content Search Engine Server software. You must install


Content Search Engine and Content Engine software on the same operating system. For example, if Content Engine runs on Windows, locate the Content Search Engine Client installation software that runs on Windows.

3. Start the installation program.

Operating System	Installation Program
AIX	P8CSE-CLIENT-4.5.1-AIX.BIN
HP-UX	P8CSE-CLIENT-4.5.1-HPUX.BIN
HP-UXi	P8CSE-CLIENT-4.5.1-HPUXi.BIN
Linux	P8CSE-CLIENT-4.5.1-LINUX.BIN
Linux on System z	P8CSE-CLIENT-4.5.1-ZLINUX.BIN
Solaris	P8CSE-CLIENT-4.5.1-SOL.BIN
Windows	P8CSE-CLIENT-4.5.1-WIN.EXE

4. Complete the Content Search Engine Client installation screens by using the values from your worksheet.
5. Review the following Content Search Engine Client log files:
 - Windows - `cse_client_install_path\CSEClient_install_log_4.5.1.0.log`
 - UNIX - `cse_client_install_path/CSEClient_install_log_4.5.1.0.log`

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 Content Search Engine Client files silently

You can install the Content Search Engine Client files silently by editing a silent input file and running the installation program from a command line. You must install Content Search Engine Client files on all application server machines where Content Engine Server is installed.

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

To install Content Search Engine Client files:

1. On the machine where Content Engine is to be deployed, log on as `ce_install_user`.
2. Locate the Content Search Engine Client installation software. It must be the same version as your Content Search Engine Server software. You must install Content Search Engine and Content Engine software on the same operating system. For example, if Content Engine runs on Windows, locate the Content Search Engine Client installation software that runs on Windows.
3. Locate the `CSE_silent_install.txt` file within the directory that contains the Content Search Engine Client installation software, and edit the file to specify the location where you want to install the Content Search Engine Client files.

The default installation paths are as follows:

UNIX `/opt/IBM/FileNet/ContentEngine/CSEClient`

Windows

`C:\Program Files\IBM\FileNet\ContentEngine\CSEClient`


4. Start the Content Search Engine Client installation program.

Operating System	Installation Program
AIX	P8CSE-CLIENT-4.5.1-AIX.BIN -f CSEClient_silent_install.txt -i silent
HP-UX	P8CSE-CLIENT-4.5.1-HPUX.BIN -f CSEClient_silent_install.txt -i silent
HP-UXi	P8CSE-CLIENT-4.5.1-HPUXi.BIN -f CSEClient_silent_install.txt -i silent
Linux	P8CSE-CLIENT-4.5.1-LINUX.BIN -f CSEClient_silent_install.txt -i silent
Linux on System z	P8CSE-CLIENT-4.5.1-ZLINUX.BIN -f CSEClient_silent_install.txt -i silent
Solaris	P8CSE-CLIENT-4.5.1-SOL.BIN -f CSEClient_silent_install.txt -i silent
Windows	P8CSE-CLIENT-4.5.1-WIN.EXE -f CSEClient_silent_install.txt -i silent

5. Review the following Content Search Engine Client log files:

- Windows - *cse_client_install_path\CSEClient_install_log_4.5.1.0.log*
- UNIX - *cse_client_install_path/CSEClient_install_log_4.5.1.0.log*

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 Process Engine Client files on Content Engine servers

Install the Process Engine Client files on the Content Engine to enable communication between Content Engine and Process Engine. You can install the files interactively by using the installation wizard or silently by using the command line and a silent input file.

“Installing the latest Process Engine Client files on Content Engine servers interactively”

The installation wizard provides an interactive way to install the Process Engine Client files. You can use the values you collected on your worksheet to fill in the required value for each field on the wizard screens.

“Installing the latest Process Engine Client files on Content Engine servers silently” on page 20

You can install the Process Engine Client software on the Content Engine server by using a silent input text file and running the installation program from the command line. Use the values in your installation worksheet to edit the silent input text file before you run the installation.

Installing the latest Process Engine Client files on Content Engine servers interactively

The installation wizard provides an interactive way to install the Process Engine Client files. You can use the values you collected on your worksheet to fill in the required value for each field on the wizard screens.

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

Except where noted, the following steps apply to IBM WebSphere Application Server, Oracle WebLogic Server, and JBoss Application Server.

To install the Process Engine Client 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 Content Engine values, filter by **PE Client Installer** in the **Installation or Configuration Program** column.


2. On the machine where Content Engine is to be deployed, log on as *ce_install_user*.
3. Locate the Process Engine Client installation software. The version of the Process Engine Client software must match the version of Process Engine software.
4. Expand the TAR or ZIP file of the Process Engine Client installation software.
5. Start the installation program by running the following command.

Operating System	Install Program
AIX	P8PE-CLIENT-PE_version-AIX.BIN
HPUX	P8PE-CLIENT-PE_version-HPUX.BIN
HPUXi	P8PE-CLIENT-PE_version-HPUXI.BIN
Linux	P8PE-CLIENT-PE_version-LINUX.BIN
Solaris	P8PE-CLIENT-PE_version-SOL.BIN
Windows	P8PE-CLIENT-PE_version-WIN.EXE
Linux on System z	P8PE-CLIENT-PE_version-ZLINUX.BIN

6. Complete the Process Engine Client installation screens by using the values from your worksheet.
7. If the Process Engine is configured to use the IPv6 network protocol, locate and edit the `taskman.properties` file and add the following lines to that file:


```
-Djava.net.preferIPv6Addresses=true
-Djava.net.preferIPv4Stack=false
```

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 Process Engine Client files on Content Engine servers silently

You can install the Process Engine Client software on the Content Engine server by using a silent input text file and running the installation program from the command line. 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.

Except where noted, the following steps apply to IBM WebSphere Application Server, Oracle WebLogic Server, and JBoss Application Server.

To install the Process Engine Client 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 Content Engine values, filter by **PE Client Installer** in the **Installation or Configuration Program** column.

2. On the machine where Content Engine is to be deployed, log on as *ce_install_user*.
3. Locate the Process Engine Client installation software. The version of the Process Engine Client software must match the version of Process Engine software.
4. Expand the TAR or ZIP file of the Process Engine Client installation software.
5. In the expanded installation software, open the file `PEClient_silent_install.txt` and make the following changes:
 - a. Change the `Variable_CheckboxCE` line to:



```
-V Variable_CheckboxCE="true"
```
 - b. Save your changes.
6. Start the installation program by running the following command:

Operating System	Install Program
AIX	<code>P8PE-CLIENT-PE_version-AIX.BIN -silent -options "PEClient_silent_install.txt"</code>
HPUX	<code>P8PE-CLIENT-PE_version-HPUX.BIN -silent -options "PEClient_silent_install.txt"</code>
HPUXi	<code>P8PE-CLIENT-PE_version-HPUXI.BIN -silent -options "PEClient_silent_install.txt"</code>
Linux	<code>P8PE-CLIENT-PE_version-LINUX.BIN -silent -options "PEClient_silent_install.txt"</code>
Solaris	<code>P8PE-CLIENT-PE_version-SOL.BIN -silent -options "PEClient_silent_install.txt"</code>
Windows	<code>P8PE-CLIENT-PE_version0-WIN.EXE -silent -options "PEClient_silent_install.txt"</code>
Linux on System z	<code>P8PE-CLIENT-PE_version-ZLINUX.BIN -silent -options "PEClient_silent_install.txt"</code>

7. If the Process Engine is configured to use the IPv6 network protocol, locate and edit the `taskman.properties` file and add the following lines to that file:


```
-Djava.net.preferIPv6Addresses=true
-Djava.net.preferIPv4Stack=false
```

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 Content Engine

You can configure and deploy all of your Content Engine instances with Configuration Manager. Configuration Manager prepares the Content Engine application for deployment on the application server. A single Content 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 Engine application environment, then you apply the settings by running the configuration tasks, and then you 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 Engine instance:

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

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

- (WebSphere Application Server only) For best results, configure no more than one Content Engine instance in a WebSphere profile.
 - If you need an accessible software version of Configuration Manager for people with disabilities, use the command-line version of Configuration Manager.
 - If your system is HP-RISC, use the command-line version of Configuration Manager.
 - If your system is Novell SUSE Linux Enterprise 9, use the command-line version of Configuration Manager.
 - 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 complete the tasks on the initial server, you copy the EAR file with the bootstrap settings to the additional servers.
1. “Resolving the names of existing data sources”
You must create data sources for the Global Configuration Data (GCD) database and your object store databases. Configuration Manager will not create a new data source with the same name as that of an existing data source. If you want to reuse a data source name, you must resolve data source naming conflicts before you configure the JDBC data sources.
 2. “Granting directory permissions to the Configuration Manager user” on page 23
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.
 3. “Configuring Content Engine instances” on page 23
You can configure and deploy all of your Content Engine instances with Configuration Manager. A single Content 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.

Resolving the names of existing data sources

You must create data sources for the Global Configuration Data (GCD) database and your object store databases. Configuration Manager will not create a new data

source with the same name as that of an existing data source. If you want to reuse a data source name, you must resolve data source naming conflicts before you configure the JDBC data sources.

Perform this procedure only if you already created data source names by using your application server administration tools and you want to use Configuration Manager to create the data sources.

To resolve data source name reuse issues:

1. Use your application server administration tools to determine if the data source names that you selected already exist.
2. If you have a duplicate data source name that you want to use, manually delete the existing data source from your application server. See your application server documentation for more information.

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. Log on as *ce_install_user* to the server where you installed Content Engine.
2. Grant permissions to the *config_mgr_user* user for the executable file that you intend to use:

Option	Description
UNIX - graphical user interface	Grant execute permission to configmgr
UNIX - command line	Grant execute permission to configmgr_cl
Windows - graphical user interface	Grant read and execute permission to configmgr.exe
Windows - command line	Grant read and execute permission to configmgr_cl.exe

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 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 Engine instances

You can configure and deploy all of your Content Engine instances with Configuration Manager. A single Content 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.

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

- (WebSphere Application Server only) For best results, configure no more than one Content Engine instance in a WebSphere profile.
- If you need an accessible software version of Configuration Manager for people with disabilities, use the command-line version of Configuration Manager.
- If your system is HP-RISC, use the command-line version of Configuration Manager.
- If your system is Novell SUSE Linux Enterprise 9, use the command-line version of Configuration Manager.
- 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 complete the tasks on the initial server, you copy the EAR file with the bootstrap settings to the additional servers.

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.
JBoss Application Server	Stop the application server.
WebLogic Server	Start the application server if it is not already running.

“Configuring Content Engine instances by using the graphical user interface”
You use the graphical user interface version of Configuration Manager to configure and deploy a Content Engine application instance on an application server.

“Configuring instances by using the command line” on page 32
You can configure a Content Engine instance on a web application server by using the command-line version of Configuration Manager.

Configuring Content Engine instances by using the graphical user interface

You use the graphical user interface version of Configuration Manager to configure and deploy a Content 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 Engine application
- The directory service provider (LDAP) settings
- The Content 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 Login Modules, Configure LDAP properties, and Configure Bootstrap 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 25
You can start the graphical interface version of Configuration Manager to configure a Content Engine application instance on a web application server.

2. “Changing the password save preference” on page 26
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 26
Configuration Manager stores your settings for deploying a Content 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 Engine bootstrap settings, and the application deployment settings. You must create a new profile for each Content Engine instance that you are configuring.
4. “Configuring the Global Configuration Data JDBC data source settings” on page 27
You must provide property information about the JDBC data sources for the Global Configuration Data (GCD) database. Content Engine uses the data source information to connect to and update the GCD database.
5. “Configuring the login modules (WebSphere and JBoss only)” on page 28
You must configure the login modules for the Content Engine application. The login modules provide authentication information for the Content Engine application.
6. “Configuring the directory service provider (LDAP) settings” on page 29
You must configure the directory service provider (LDAP) settings. The directory service provider (LDAP) settings define the directory service and the users and groups that Content Engine uses for authentication.
7. “Configuring the bootstrap settings” on page 30
You must configure the bootstrap settings. The bootstrap information is needed for creating the Global Configuration Data (GCD) and for starting Content Engine.

Starting the Configuration Manager graphical user interface:

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

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 Engine:

Option	Description
UNIX	Run this command: <code>ce_install_path/tools/configure/configmgr</code>
Windows	Perform one of the following actions: <ul style="list-style-type: none"> • Double-click the FileNet Configuration Manager desktop shortcut. • Click Start → All Programs → IBM FileNet P8 Platform → FileNet Configuration Manager. • Run the following command: <code>ce_install_path\tools\configure\configmgr.exe</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, you must specify any passwords required by the tasks and for the application server properties before you run the tasks; otherwise, the tasks won't 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 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 Engine bootstrap settings, and the application deployment settings. You must create a new profile for each Content 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 Engine is installed. For more information on profiles, see “Configuration profile concepts” on page 532.

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.
4. 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*.

Related tasks

“Configuration Manager user interface reference” on page 538

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content 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.

Configuring the Global Configuration Data JDBC data source settings:

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

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

Table 3. Required application server state

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


To configure the JDBC 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 GCD JDBC Data Sources** 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 GCD JDBC Data Sources** in the profile pane and select **Edit Selected Task**.
4. Enter the property values for your database by using the values in your worksheet.
5. 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.
6. Select **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 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*.

Related tasks

“Configuration Manager user interface reference” on page 538

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content 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.

Configuring the login modules (WebSphere and JBoss only):

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

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

Table 4. Required application server state

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


Table 4. Required application server state (continued)

Option	Description
JBoss Application Server	Stop the application server.

To configure the login module settings:

1. If your configuration profile is not open in Configuration Manager, open the profile.
2. 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 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

“Configuration Manager user interface reference” on page 538

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content 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.

Configuring the directory service provider (LDAP) settings:

You must configure the directory service provider (LDAP) settings. The directory service provider (LDAP) settings define the directory service and the users and groups that Content Engine uses for authentication.

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

If you plan to configure Content 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 **System Administration** → **Enterprise-wide Administration** → **FileNet P8 Security** → **How to...** → **Configuration Content Engine to use e-mail or UPN for login**.

Restriction: JBoss Application Server only. Do not use Configuration Manager to configure multiple LDAP realms. Use IBM FileNet Enterprise Manager to configure multiple realms, as instructed in the IBM FileNet P8 help topic **System Administration** → **Enterprise-wide Administration** → **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 **File** → **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.

Oracle WebLogic Server only. When you run the **Configure LDAP** task, the `weblogic.security.providers.authentication.DefaultAuthenticator.ControlFlag` value is set to `SUFFICIENT` for authenticating users.

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

“Configuration Manager user interface reference” on page 538

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content 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.

Configuring the bootstrap settings:

You must configure the bootstrap settings. The bootstrap information is needed for creating the Global Configuration Data (GCD) and for starting Content Engine.

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

If you plan to configure Content Engine to use the directory server's e-mail 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 bootstrap settings. For detailed steps, see the IBM FileNet P8 help topic **System Administration → Enterprise-wide Administration → FileNet P8 Security → How to... → Configuration Content Engine to use e-mail or UPN for login.**

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 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** 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 Properties (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 bootstrap property settings by right-clicking **Configure bootstrap properties** 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 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 each additional Content Engine server.

install_dir

The location where Content 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: Only run the **Configure bootstrap properties** task 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*.

Related tasks

“Configuration Manager user interface reference” on page 538

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content 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.

Configuring instances by using the command line

You can configure a Content 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 Data (GCD) data source JDBC data source settings, the login modules for the Content Engine application, the directory service provider (LDAP) settings, and the Content 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 Engine application. If you are deploying multiple Content 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 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.
2. “Editing the configuration XML files for a Content Engine instance” on page 39
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.
3. “Running the configuration XML files” on page 42
Running the configuration XML files applies the settings. You use the **execute** command to apply your configuration settings from the command line.
4. “Checking the completion status of Content Engine configuration tasks” on page 46
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 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 Engine instance.

Table 5. 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 Data (GCD) and starting Content Engine.
configurejdbcgcd.xml	Settings for configuring JDBC connections to the databases used by Content Engine. You must generate, edit, and run the configure the JDBC task once for the data sources for the Global Configuration Data (GCD) and then again for the data sources for each object store. For information about creating the additional data sources for the object store, see “Creating the data sources by using the command line” on page 74. 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.
configurejdbcgos.xml	
configurejdbcos.n.xml , where <i>n</i> is an integer starting with 2	
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.n.xml , where <i>n</i> is an integer starting with 2	
configureloginmodules.xml	Settings for creating the application server login modules for Content Engine.

You must eventually generate each of the required configuration XML files to configure a Content 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 Engine at the same time with a single command.

“Generating one configuration XML file at a time (WebSphere)” on page 35

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

“Generating one configuration XML file at a time (WebLogic or JBoss)” on page 37

From the command line, you can generate each of the required configuration XML files for Content 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 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 application 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 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
```

Oracle WebLogic Server or JBoss Application Server

```
configmgr_cl generateconfig -appserver app_server_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* or *configurejdbcos* option. This parameter specifies the type of database to be used by Content 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 Engine uses for authenticating users and must be *activedirectory*, *adam*, *edirectory*, *oid*, *sunjava*, 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 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 Engine deployment. The value must be `standard`, `cluster`, or `netdeploy` (network deployment).

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

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

To generate a single configuration XML file:

1. Log on to the application server as `config_mgr_user`, which is 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 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 Engine uses for authenticating users and must be `activedirectory`, `adam`, `edirectory`, `oid`, `sunjava`, 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 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 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.

Generating one configuration XML file at a time (WebLogic or JBoss):

From the command line, you can generate each of the required configuration XML files for Content 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 Data (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.

To generate a single configuration XML file:

1. Log on to the application server as *config_mgr_user*, which is 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.

Oracle WebLogic Server or JBoss Application Server only. Generate the *configurebootstrap.xml* file for the *configurebootstrap* task:

```
configmgr_cl generateconfig -appserver app_server_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
-db db_type -task configurejdbcgcd -profile myprofile
```

Generate the *configurejdbcos.n.xml* file for the *configurejdbcos* task for the data sources for a single object store:

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

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

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

JBoss only. Generate the *configureloginmodules.xml* file for the *configureloginmodules* task:

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

where:

-appserver *appserver_name*

-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 files by using the *configurejdbcgcd* or *configurejdbcos* option. This parameter specifies the type of database to be used by Content 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 Engine uses for authenticating users and must be *activedirectory*, *adam*, *edirectory*, *oid*, *sunjava*, 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 operation for the profile and must be *new*, *modify*, or *upgrade*.

-profile *myprofile*

The **-profile** *myprofile* parameter specifies the profile to use. Use one of the following values for *myprofile*:

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

Editing the configuration XML files for a Content 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 Engine to use the directory server's e-mail 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 IBM FileNet P8 help topic **System Administration** → **Enterprise-wide Administration** → **FileNet P8 Security** → **How to...** → **Configuration Content Engine to use e-mail or UPN for login**.

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 each 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 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 Data (GCD)
 - `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 Global Configuration Data (GCD) database, 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 database.
5. Save your edits and close the XML file.
6. Optional: Add encrypted passwords to the XML files by running the `storepasswords` command.

- a. Enter the following command on one line:


```
configmgr_c1 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 Engine settings affected by the task.

Table 6. *task_type* values

Task	Configuration file	Description
omitted	<code>applicationserver.xml</code> <code>configurebootstrap.xml</code> <code>configurejdbc.xml</code> <code>configureldap.xml</code> <code>deployapplication.xml</code>	When you omit the <code>-task task_type</code> 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.
<code>configurebootstrap</code>	<code>configurebootstrap.xml</code>	Encrypts the password for the <code>BootstrapPassword</code> property that is used to create the Global Configuration Data and to start Content Engine.

Table 6. *task_type* values (continued)

Task	Configuration file	Description
configurejdbcgcd	configurejdbcgcd.xml	Encrypts the password for the DatabasePassword property that Content 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 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.
configureldap	configureldap.xml configureldap. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Encrypts the password for the LDAPBindPassword property that Content Engine uses to connect to the directory server for authenticating Content Engine users. If you have more than one configureldap. <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 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 edit 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 535 for more information.

To run the configuration XML files:

1. Start or stop the application server.

Option	Description
WebSphere Application Server	Start the application server if it is not already running.
JBoss Application Server	Stop the application server.
Oracle WebLogic Server	Start the application server 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"

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

"Running one configuration XML file at a time" on page 43

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 Engine configuration.

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 Engine at the same time with a single command. Any configuration XML file that has the <TaskEnabled> 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 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 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 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 each additional Content Engine server.

install_dir

The location where Content 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.

Oracle WebLogic Server only. When you run all the tasks, the `weblogic.security.providers.authentication.DefaultAuthenticator.ControlFlag` value is set to `SUFFICIENT` for authenticating users.

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 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 535 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 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 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 Engine server.

- Configure the JDBC Data Sources for the Global Configuration Data (GCD) database 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.
Oracle WebLogic Server only. When you run the task using the `configureldap` option, the `weblogic.security.providers.authentication.DefaultAuthenticator.ControlFlag` value is set to `SUFFICIENT` for authenticating users.
- 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 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 task_file_name  
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 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 Global Configuration Data (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 each additional Content Engine server.

install_dir

The location where Content 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 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 7. 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 47

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 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 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 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 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 2 on page 47 as needed to check status on one of the other configuration XML files.

The task execution status messages are displayed.

Deploying Content Engine instances

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

Perform the procedures in this topic after you have performed the configuration tasks in "Configuring Content Engine" on page 21 and you have installed the latest version of the Process Engine client files on the Content Engine.

Restriction: Use the command line version of Configuration Manager if either of these conditions is true:

- Your system is Novell SUSE Linux Enterprise 9. You can configure Content Engine only with the command line.
- You need an accessible software version of Configuration Manager for people with disabilities to use.

"Deploying instances by using the graphical user interface" on page 49

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

“Deploying Content Engine by using the Configuration Manager command line” on page 50

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

“Deploying Content Engine to additional JBoss servers in a cluster” on page 54
Use the following procedure to deploy a Content Engine Server instance on each additional JBoss Application Server in your cluster.

Deploying instances by using the graphical user interface

You can deploy a Content Engine Server instance on the web application server by using the graphical user interface. Deploying makes the Content 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 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
UNIX	Type the following command: <i>ce_install_path/tools/configure/configmgr</i> where <i>ce_install_path</i> is the location where the Content Engine server software is installed
Windows	Complete one of the following actions: <ul style="list-style-type: none"> • Double-click the FileNet Configuration Manager desktop shortcut. • Select Start → All Programs → IBM FileNet P8 Platform → FileNet Configuration Manager. • Run <i>ce_install_path\tools\configure\configmgr.exe</i>. where <i>ce_install_path</i> is the location where the Content Engine server software is installed

4. Select **File** → **Open Configuration Profile**.

5. Enter the path to the profile for this Content Engine instance, or click **Browse** to locate the *profilename.cfgp* 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. Select **File** → **Save**.
10. 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.
11. 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

“Configuration Manager user interface reference” on page 538

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content 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.

 [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*.

Deploying Content Engine by using the Configuration Manager command line

From the command line you can deploy the Content 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 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” on page 51
The `deployapplication.xml` file contains settings for deploying the Content Engine application. You must use the **generateConfig** command to create the XML file.
2. “Editing the deployment configuration files” on page 52
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 53
From the command line, you can run the **execute** command on the `deployapplication.xml` configuration XML file to deploy the Content Engine application on the web application server.
4. “Checking the configuration status of the `deployapplication` task” on page 53
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 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 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 Engine deployment. The value must be `standard`, `cluster`, or `netdeploy` (network deployment).

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

Specify `netdeploy` if you are deploying Content Engine to a managed WebSphere Application Server instance. That is, you are using Network Deployment to manage individual servers that are not necessarily 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 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 Engine" on page 21, 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.
 - 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 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
```

### 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 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 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 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`".

### 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 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 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.

## Deploying Content Engine to additional JBoss servers in a cluster

Use the following procedure to deploy a Content Engine Server instance on each additional JBoss Application Server in your cluster.

**Important:** Because JBoss clusters communicate state over multicast, it is critical that you configure clusters for Content Engine to segregate multicast traffic from each other and from other JBoss clusters. You can find instructions regarding JBoss cluster configuration at <http://www.jboss.com>.

To deploy Content Engine Server on additional JBoss servers in a cluster:

1. Leave Content Engine deployed on the application server where you installed it.
2. Copy the following files from the initial Content Engine instance to each JBoss node you are setting up:
  - All data source (`JBoss_HOME/server/all/deploy/*-ds.xml`) files created as part of the configuration process.

**Important:** Depending on how you installed JBoss, there might be data source files not created by Configuration Manager, such as `hsqldb-ds.xml`, in the same location. Do not copy these files.

- `JBoss_HOME/server/all/deploy/Engine-ds.xml`
- The JDBC driver in `JBoss_HOME/server/all/lib`
- `JBoss_HOME/server/all/conf/login-config.xml`
- `JBoss_HOME/server/all/deploy/Engine-jbc.ear`



**Tip:** Clustered JBoss instances are deployed from the "all" directory and not the "default" directory. You can find instructions regarding JBoss cluster configurations at <http://www.jboss.com>

3. Start or restart the application server.
4. Verify that the `server.log` file located in the `JBOSS_home/server/all/log` directory lists deployment of the WAR or EAR file you used. If it does, then the deployment of Content Engine is successful.

---

## Installing storage device source files

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

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

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 and adding native API library paths (WebLogic)” on page 56

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 and adding native API library paths (JBoss)” on page 59

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 61

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

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

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 Engine is deployed.

“Copying the Tivoli Storage Manager API libraries to additional servers” on page 56

If you are running a Content 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 56

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 Engine is deployed.

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 fixed content device in FileNet Enterprise Manager. If you are installing Tivoli Storage Manager client on multiple UNIX hosts, the installation path must be the same on each host. On AIX, install Tivoli Storage Manager client at `/usr/tivoli/tsm/client/ba/bin`.

### Copying the Tivoli Storage Manager API libraries to additional servers

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

Copy the entire `tsm100` directory structure from the Content 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                                                    |
|---------|----------------------------------------------------------------|
| UNIX    | <code>/opt/IBM/FileNet/ContentEngine/tsm100</code>             |
| Windows | <code>C:\Program Files\IBM\FileNet\ContentEngine\tsm100</code> |

### 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.

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. For the detailed procedure on creating the shared library, visit <http://www.ibm.com/software/webservers/appserv/was/library/>.
  - 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`.

## Installing Tivoli Storage Manager client and adding native API library paths (WebLogic)

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” on page 57

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

“Copying the Tivoli Storage Manager API library files to additional servers” on page 57

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

“Creating a shared library definition for Tivoli Storage Manager native API library files” on page 57

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 Engine is deployed.

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 fixed content device in FileNet Enterprise Manager. If you are installing Tivoli Storage Manager client on multiple UNIX hosts, the installation path must be the same on each host. On AIX, install Tivoli Storage Manager client at `/usr/tivoli/tsm/client/ba/bin`.

## Copying the Tivoli Storage Manager API library files to additional servers

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

Copy the entire `tsm100` directory structure from the Content 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                                                    |
|---------|----------------------------------------------------------------|
| UNIX    | <code>/opt/IBM/FileNet/ContentEngine/tsm100</code>             |
| Windows | <code>C:\Program Files\IBM\FileNet\ContentEngine\tsm100</code> |

## 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.

1. Open in an edit window the WebLogic script that sets up the domain environment. The following are example paths to this script:

| Option  | Description                                                                 |
|---------|-----------------------------------------------------------------------------|
| UNIX    | <code>/opt/bea/user_projects/domains/base_domain/bin/setDomainEnv.sh</code> |
| Windows | <code>C:\bea\user_projects\domains\base_domain\bin\setDomainEnv.cmd</code>  |

2. Edit the WebLogic script by adding the lines shown below, for your operating system, just before the line in which the `WL_HOME` variable is set. Substitute your version identifier in place of `weblogic92` as appropriate. There is no carriage return after any line that ends with `/`, `\`, `;`, or `_`.

| Option                           | Description                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AIX</b>                       | TSMAPILIB=/opt/IBM/FileNet/<br>ContentEngine/tsm100<br>LIBPATH=\${LIBPATH}:\${TSMAPILIB}<br>EXT_POST_CLASSPATH=<br>\${EXT_POST_CLASSPATH}:<br>\${TSMAPILIB}/TsmJavaApi.jar<br>export LIBPATH EXT_POST_CLASSPATH<br>WL_HOME="/opt/bea/weblogic92"<br>export WL_HOME                                                                                                         |
| <b>HP-UX (32-bit)</b>            | TSMAPILIB=/opt/IBM/FileNet/<br>ContentEngine/tsm100<br>SHLIB_PATH=\${SHLIB_PATH}:\${TSMAPILIB}<br>EXT_POST_CLASSPATH=<br>\${EXT_POST_CLASSPATH}:<br>\${TSMAPILIB}/TsmJavaApi.jar<br>export SHLIB_PATH EXT_POST_CLASSPATH<br>WL_HOME="/opt/bea/weblogic92"<br>export WL_HOME                                                                                                |
| <b>HP-UX (64-bit) and HP-UXi</b> | TSMAPILIB=/opt/IBM/FileNet/<br>ContentEngine/tsm100<br>SHLIB_PATH=\${SHLIB_PATH}:\${TSMAPILIB}<br>EXT_POST_CLASSPATH=<br>\${EXT_POST_CLASSPATH}:<br>\${TSMAPILIB}/TsmJavaApi.jar<br>export SHLIB_PATH EXT_POST_CLASSPATH<br>JAVA_OPTIONS="\${JAVA_OPTIONS} -d64"<br>export JAVA_OPTIONS<br>WL_HOME="/opt/bea/weblogic92"<br>export WL_HOME                                 |
| <b>Linux</b>                     | TSMAPILIB=/opt/IBM/FileNet/<br>ContentEngine/tsm100<br>LD_LIBRARY_PATH=\${LD_LIBRARY_PATH}:<br>\${TSMAPILIB}<br>EXT_POST_CLASSPATH=<br>\${EXT_POST_CLASSPATH}:<br>\${TSMAPILIB}/TsmJavaApi.jar<br>export LD_LIBRARY_PATH EXT_<br>POST_CLASSPATH<br>WL_HOME="/opt/bea/weblogic92"<br>export WL_HOME                                                                         |
| <b>Solaris (32-bit)</b>          | TSMAPILIB=/opt/IBM/FileNet/<br>ContentEngine/tsm100<br>TSMCLIENTLIB=/opt/tivoli/tsm/client/<br>api/bin<br>LD_LIBRARY_PATH=\${LD_LIBRARY_PATH}:<br>\${TSMAPILIB}:<br>\${TSMCLIENTLIB}<br>EXT_POST_CLASSPATH=<br>\${EXT_POST_CLASSPATH}:<br>\${TSMAPILIB}/TsmJavaApi.jar<br>export LD_LIBRARY_PATH EXT_<br>POST_CLASSPATH<br>WL_HOME="/opt/bea/weblogic92"<br>export WL_HOME |

| Option           | Description                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Solaris (64-bit) | <pre>TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 TSMCLIENTLIB=/opt/tivoli/tsm/client/ api/bin64 LD_LIBRARY_PATH_64= \${LD_LIBRARY_PATH_64}: \${TSMAPILIB}:\${TSMCLIENTLIB} EXT_POST_CLASSPATH= \${EXT_POST_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export LD_LIBRARY_PATH_64 EXT_POST_ CLASSPATH JAVA_OPTIONS="\${JAVA_OPTIONS} -d64" export JAVA_OPTIONS WL_HOME="/opt/bea/weblogic92" export WL_HOME</pre> |
| Windows          | <pre>set TSMAPILIB=C:\\Program Files\\IBM\\ FileNet\\ContentEngine\\tsm100 set PATH=%PATH%;%TSMAPILIB% set EXT_POST_CLASSPATH=%EXT_POST_ CLASSPATH%;%TSMAPILIB%\\TsmJavaApi.jar set WL_HOME=C:\\bea\\weblogic92</pre>                                                                                                                                                                                              |

3. If you are using WebLogic Node Manager to start and stop WebLogic Managed Servers in a clustered environment, you must enable Node Manager to use the appropriate start script:
  - a. Open for editing the node manager configuration file WL\_HOME/common/nodemanager/nodemanager.properties.
  - b. Set the StartScriptEnabled property to true (default is false).
  - c. Set the StartScriptName to match the script name used by Node Manager to start the managed server, depending on your operating system:

| Option  | Description                              |
|---------|------------------------------------------|
| UNIX    | StartScriptName=startManagedWebLogic.sh  |
| Windows | StartScriptName=startManagedWebLogic.cmd |

**Important:** If the managed server is not on the same machine as the WebLogic Administration Server and you have an alternate script matching the name of the Managed Server in the domain bin directory, make sure to specify that script name instead of the more generic "startManagedWebLogic" script.

4. Save your edits in nodemanager.properties and restart the Node Manager.

## Installing Tivoli Storage Manager client and adding native API library paths (JBoss)

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” on page 60

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

“Copying the Tivoli Storage Manager API libraries to additional servers” on page 60

If you are running a Content 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”

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 Engine is deployed.

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 fixed content device in FileNet Enterprise Manager. If you are installing Tivoli Storage Manager client on multiple UNIX hosts, the installation path must be the same on each host. On AIX, install Tivoli Storage Manager client at `/usr/tivoli/tsm/client/ba/bin`.

## Copying the Tivoli Storage Manager API libraries to additional servers

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

Copy the entire `tsm100` directory structure from the Content 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                                                    |
|---------|----------------------------------------------------------------|
| UNIX    | <code>/opt/IBM/FileNet/ContentEngine/tsm100</code>             |
| Windows | <code>C:\Program Files\IBM\FileNet\ContentEngine\tsm100</code> |

## 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.

1. Open in an edit window the JBoss startup script that sets up the domain environment:

| Option  | Description          |
|---------|----------------------|
| UNIX    | <code>run.sh</code>  |
| Windows | <code>run.bat</code> |

2. Edit the startup script by adding the following lines at the start of the script. There is no carriage return after any line that ends with `/`, `\`, `:`, or `_`

| Option | Description                                                                                                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AIX    | <code>TSMAPILIB=/opt/IBM/FileNet/ContentEngine/tsm100<br/>LIBPATH=\${LIBPATH}:\${TSMAPILIB}<br/>JBOSS_CLASSPATH=\${JBOSS_CLASSPATH}:<br/>\${TSMAPILIB}/TsmJavaApi.jar<br/>export LIBPATH JBOSS_CLASSPATH</code> |

| Option                           | Description                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HP-UX (32-bit)</b>            | TSMAPILIB=/opt/IBM/FileNet/<br>ContentEngine/tsm100<br>TSMCLIENTLIB=/opt/tivoli/tsm/client/<br>api/bin64<br>SHLIB_PATH=\${SHLIB_PATH}:\${TSMAPILIB}:<br>\${TSMCLIENTLIB}<br>JBOSS_CLASSPATH=\${JBOSS_CLASSPATH}:<br>\${TSMAPILIB}/TsmJavaApi.jar<br>export SHLIB_PATH JBOSS_CLASSPATH                                                                                  |
| <b>HP-UX (64-bit) and HP-UXi</b> | TSMAPILIB=/opt/IBM/FileNet/<br>ContentEngine/tsm100<br>TSMCLIENTLIB=/opt/tivoli/tsm/client/<br>api/bin64<br>SHLIB_PATH=\${SHLIB_PATH}:\${TSMAPILIB}:<br>\${TSMCLIENTLIB}<br>JBOSS_CLASSPATH=\${JBOSS_CLASSPATH}:<br>\${TSMAPILIB}/TsmJavaApi.jar<br>export SHLIB_PATH JBOSS_CLASSPATH<br>JAVA_OPTS="\${JAVA_OPTS} -d64"<br>export JAVA_OPTS                            |
| <b>Linux</b>                     | TSMAPILIB=/opt/IBM/FileNet/<br>ContentEngine/tsm100<br>LD_LIBRARY_PATH=\${LD_LIBRARY_PATH}:<br>\${TSMAPILIB}<br>JBOSS_CLASSPATH=\${JBOSS_CLASSPATH}:<br>\${TSMAPILIB}/TsmJavaApi.jar<br>export LD_LIBRARY_PATH JBOSS_CLASSPATH                                                                                                                                         |
| <b>Solaris (32-bit)</b>          | TSMAPILIB=/opt/IBM/FileNet/<br>ContentEngine/tsm100<br>TSMCLIENTLIB=/opt/tivoli/tsm/client/<br>api/binLD_LIBRARY_PATH=\${<br>LD_LIBRARY_PATH}:<br>\${TSMAPILIB}:\${TSMCLIENTLIB}<br>JBOSS_CLASSPATH=\${JBOSS_CLASSPATH}:<br>\${TSMAPILIB}/TsmJavaApi.jar<br>export LD_LIBRARY_PATH JBOSS_CLASSPATH                                                                     |
| <b>Solaris (64-bit)</b>          | TSMAPILIB=/opt/IBM/FileNet/<br>ContentEngine/tsm100<br>TSMCLIENTLIB=/opt/tivoli/tsm/client/<br>api/bin64<br>LD_LIBRARY_PATH_64=\${LD_LIBRARY_<br>PATH_64}:\${TSMAPILIB}:\${TSMCLIENTLIB}<br>JBOSS_CLASSPATH=\${JBOSS_CLASSPATH}:<br>\${TSMAPILIB}/TsmJavaApi.jar<br>export LD_LIBRARY_PATH_64<br>JBOSS_CLASSPATH<br>JAVA_OPTS="\${JAVA_OPTS} -d64"<br>export JAVA_OPTS |
| <b>Windows</b>                   | set TSMAPILIB=C:\\Program Files\\IBM<br>\\FileNet\<br>ContentEngine\\tsm100<br>set PATH=%PATH%;%TSMAPILIB%<br>set JBOSS_CLASSPATH=%JBOSS_CLASSPATH%;<br>%TSMAPILIB%\\TsmJavaApi.jar                                                                                                                                                                                    |

## Installing or updating EMC Centera SDK library files

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

“Installing EMC Centera SDK version 3.2 library files”

Content Engine needs to use the SDK library files to access EMC Centera fixed content devices.

“Configuring EMC Centera SDK environment variables for version 3.2” on page 63

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

### Installing EMC Centera SDK version 3.2 library files

Content Engine needs to use the SDK library files to access EMC Centera fixed content devices.

To install EMC Centera SDK version 3.2 library files:

1. Log on to the Content Engine Server machine as *ce\_install\_user*.
2. Back up or delete any existing EMC Centera SDK library files, which are located in the Default Destination Installation Location column of the following table:

| Operating system | Default destination installation location |
|------------------|-------------------------------------------|
| AIX              | /usr/local/Centera_SDK                    |
| HP-UX            | /opt/Centera_SDK                          |
| Linux            | /usr/local/Centera_SDK                    |
| Solaris          | /opt/Centera_SDK                          |
| Windows          | C:\Centera_SDK                            |

3. Copy the appropriate directory to a location on the Content Engine Server machine, such as /tmp (UNIX) or C:\Temp (Windows), as shown in the following table. The Centera directory in the Content Engine software package contains the Centera SDK version 3.2 installation files.

| Operating system      | Directory to be copied                                                                                                                                                                                                                         |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AIX, Solaris, Windows | Copy the entire Centera directory                                                                                                                                                                                                              |
| HP-UX 11i v1 (11.11)  | Copy Centera/11i-v1-11.11                                                                                                                                                                                                                      |
| HP-UX 11i v2 (11.23)  | Copy Centera/11iv1-11.23                                                                                                                                                                                                                       |
| Linux                 | Depending on the version of GCC (GNU Compiler Collection) on the application server machine, copy one of the following directories:<br><div style="margin-left: 40px;">Centera/gcc3.3</div> <div style="margin-left: 40px;">Centera/gcc4</div> |

4. On the Content 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 Engine Server machine. On UNIX, the installer script prompts you for the install directory. On Windows, specify the installation directory, such as `C:\Centera_SDK`, on the command line.

| Option | Description             |
|--------|-------------------------|
| UNIX   | <code>install.sh</code> |



| Option  | Description                |
|---------|----------------------------|
| Windows | install.bat C:\Centera_SDK |

6. The installer script creates both 32-bit and 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.

| Operating system          | Subdirectories of extracted EMC Centera SDK directory | Description                                                |
|---------------------------|-------------------------------------------------------|------------------------------------------------------------|
| AIX, Solaris, and Windows | lib                                                   | lib has the native library files that are to be installed. |
| HP-UX                     | ../11i-v1-11.11/lib                                   |                                                            |
| HP-UXi                    | ../11i-v1-11.13/lib                                   |                                                            |
| Linux                     | ../gcc3.3/lib<br>../gcc4/lib                          |                                                            |

### Configuring EMC Centera SDK environment variables for version 3.2

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

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

| Option  | Description           |
|---------|-----------------------|
| UNIX    | setCenteraLibPath.sh  |
| Windows | setCenteraLibPath.bat |

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

Note that the CENTERA\_LIB\_PATH variable needs to point to the sample script, not just the installation directory that contains the script.

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/SDK3.2.607`

then change the installation path of the AIX script to:

`/usr/local/Centera/SDK3.2.607/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.

| Operating System | Script Revisions                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AIX              | <p>From:</p> <pre>CENTERA_LIB_PATH=/usr/local/Centera_SDK/lib/32 LIBPATH=\$LIBPATH:\$CENTERA_LIB_PATH export LIBPATH</pre> <p>to:</p> <pre>CENTERA_LIB_PATH= install_path /lib/32</pre> <p>or:</p> <pre>CENTERA_LIB_PATH= install_path /lib/64</pre>                                                                                                                                                                                  |
| Solaris          | <p>From:</p> <pre>CENTERA_LIB_PATH=/opt/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>      |
| Linux            | <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> |

| Operating System | Script Revisions                                                                                                                                                                                                                                                                                                                                                              |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HP-UX HP-UXi     | <p>From:</p> <pre>CENTERA_LIB_PATH=/opt/Centera_SDK/lib/32 SHLIB_PATH=\$SHLIB_PATH:\$CENTERA_LIB_PATH export SHLIB_PATH</pre> <p>to:</p> <pre>CENTERA_LIB_PATH=install_path/lib/32 SHLIB_PATH=\$SHLIB_PATH:\$CENTERA_LIB_PATH export SHLIB_PATH</pre> <p>or:</p> <pre>CENTERA_LIB_PATH=install_path/lib/64 SHLIB_PATH=\$SHLIB_PATH:\$CENTERA_LIB_PATH export SHLIB_PATH</pre> |
| Windows          | <p>From:</p> <pre>set CENTERA_LIB_PATH=C:\Centera_SDK\lib\32 set PATH=%PATH%;%CENTERA_LIB_PATH%</pre> <p>to:</p> <pre>set CENTERA_LIB_PATH=install_path \lib\32 set PATH=%PATH%;%CENTERA_LIB_PATH%</pre> <p>or:</p> <pre>set CENTERA_LIB_PATH=install_path \lib\64 set PATH=%PATH%;%CENTERA_LIB_PATH%</pre>                                                                   |

- 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.

| Application Server           | Startup Script (UNIX) | Startup Script (Windows) |
|------------------------------|-----------------------|--------------------------|
| WebSphere Application Server | setupCmdLine.sh       | setupCmdLine.cmd         |
| Oracle WebLogic Server       | setDomainEnv.sh       | setDomainEnv.cmd         |
| JBoss Application Server     | run.sh                | run.cmd                  |

- Stop and start the application server.

## Completing Content Engine post-deployment steps

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

“Completing Content Engine post-deployment steps (WebSphere)” on page 66  
You must complete the post-deployment web application server configuration before you can put an IBM FileNet P8 system into production.

“Completing Content Engine post-deployment steps (Oracle WebLogic Server)” on page 67

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

“Completing Content Engine post-deployment steps (JBoss Application Server)” on page 67

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

## Completing Content Engine post-deployment steps (WebSphere)

You must complete the post-deployment web application server configuration before you can put an IBM 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** → **Secure administration, applications, and infrastructure**.
3. If you configured Content 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 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 Engine cannot start or process requests.
5. Complete the following substeps to verify that the HTTP port used by the Content 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 where Content Engine is deployed, as follows:

| Option                    | Description                                                                                                                     |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Stand-alone server</b> | Stop and start the application server.                                                                                          |
| <b>Network Deployment</b> | Stop and start the application server where Content Engine is deployed, including the Deployment Manager and all managed nodes. |
| <b>Cluster</b>            | Stop and start the cluster.                                                                                                     |

## Completing Content Engine post-deployment steps (Oracle WebLogic Server)

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

To complete the post-deployment configuration:

Restart the web application server where Content Engine is deployed.

| Option             | Description                            |
|--------------------|----------------------------------------|
| Stand-alone server | Stop and start the application server. |
| Cluster            | Stop and start the cluster.            |

## Completing Content Engine post-deployment steps (JBoss Application Server)

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

To complete the post-deployment configuration:

1. (Windows Active Directory and JBoss 4 only.) Edit the login-config.xml file.
  - a. Make a backup copy of the login-config.xml file. The path to this file depends on the JBoss environment:

Table 8. Path to the login-config.xml file

| Environment | Path                                                            |
|-------------|-----------------------------------------------------------------|
| Standard    | <i>jboss_install_dir</i> /server/myserver/conf/login-config.xml |
| Cluster     | <i>jboss_install_dir</i> /server/all/conf/login-config.xml      |

- b. Open the login-config.xml file in a text editor.
  - c. Locate the following line inside the scope of the <login-module> element in the file:

```
<login-module code="org.jboss.security.auth.spi.LdapExtLoginModule" flag="sufficient">
```
  - d. Add the following line immediately after the <login-module> line. Do not type any line breaks.

```
<module-option name="java.naming.referral">follow</module-option>
```
  - e. Save your changes.
2. (All operating systems and all JBoss versions) Start the web application server.

---

## Verifying the Content Engine deployment

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

1. Verify the state of Content Engine deployment by browsing to the IBM FileNet P8 System Health page:  
`http://server:port/P8CE/Health`  
where:

*server* is the host name of the machine where Content Engine is deployed.  
*port* is the WSI port used by the Web application server on the machine where Content Engine is deployed.

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

Table 9. Example FileNet P8 System Health page address

Application Server Type	Web Page Address
IBM WebSphere Application Server	<a href="http://server:9080/P8CE/Health">http://server:9080/P8CE/Health</a>
Oracle WebLogic Server	<a href="http://server:7001/P8CE/Health">http://server:7001/P8CE/Health</a>
JBoss Application Server	<a href="http://server:8080/P8CE/Health">http://server:8080/P8CE/Health</a>

- Verify that the FileNet P8 System Health page contains the Content 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. In particular, if you are upgrading from version 3.5.2, a red icon appears before the GCD, directory configurations, object stores, storage areas, and sites entries. Also, if you are upgrading from version 3.5.2, no domain name appears yet in the Domain entry.

Table 10. FileNet P8 System Health page contents

Section	Description
<b>Domain</b>	Displays the FileNet P8 domain name if a domain was found.
<b>Global Configuration Database</b>	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.
<b>Directory Configurations</b>	Verifies that at least one directory service is configured and lists the number of configured directory service providers.
<b>PE Connection Points</b>	Displays the number of Process Engine connection points.
<b>PE Isolated Regions</b>	Displays the number of Process Engine isolated regions.
<b>Fixed Content Devices</b>	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.
<b>Object Stores</b>	Verifies that at least one object store exists and lists the number of object stores.
<b>Storage Areas</b>	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.
<b>Content Cache Areas</b>	Displays the number of content cache areas.
<b>Sites</b>	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.

- Optional: Bookmark the FileNet P8 System Health page Web page address in your browser for later use.
- Browse to the FileNet Engine Web page:  
<http://server:port/FileNet/Engine>

where:

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

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

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

Table 11. Example FileNet Engine Web page address

Application Server Type	Web Page Address
IBM WebSphere Application Server	http://myserver:9080/FileNet/Engine
Oracle WebLogic Server	http://myserver:7001/FileNet/Engine
JBoss Application Server	http://myserver:8080/FileNet/Engine

5. Verify that the FileNet Engine Web page contains the following information:
  - Verify the value in the **Startup Message** key. The Content Engine build and version (for example, dap451.097), 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 Engine software is installed.
  - Verify the value in the **Process Engine** key. The Process Engine Client build and version (for example, pui451.075), must match the build and version in the *version.txt* file in the TAR or ZIP file of the Process Engine Client installation software.
  - Verify that the values for JDBC driver, server instance, operating system, and other properties match the values that you entered when you configured Content Engine.
6. Optional: Bookmark the FileNet Engine Web page in your browser for later use.

---

## Establishing the FileNet P8 domain and Global Configuration Data (GCD)

With Content Engine installed and deployed, you must use IBM FileNet Enterprise Manager to create a FileNet P8 domain. You can also use Enterprise Manager to set a URL to the FileNet P8 online help if you did not specify the location when you ran the Content Engine installation program.

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

**Important:** If you run Enterprise Manager as a limited (non-administrative) user account, you cannot update the **Base URL for the FileNet P8 Platform help files** field in the General tab of the Enterprise Manager Properties dialog box. However, you can update the field later by logging on to Enterprise Manager as the *gcd\_admin* user.

1. Create a FileNet P8 domain:
  - a. 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 Enterprise Manager values for this task, filter by **EM: Create FileNet P8 domain** in the **Installation or Configuration Program** column.
  - b. Start Enterprise Manager by double-clicking the Enterprise Manager icon on the desktop, or by clicking **Start → All Programs → IBM FileNet P8 Platform → Enterprise Manager Administration Tool**.



- c. Complete the wizard screens by using the values in your worksheet. The values displayed in the screens are default values that you must change to match your site.
2. Configure directory service authentication.

**Important:** For multi-realm authorization, run the Create a Directory Configuration wizard once for each realm. See the IBM FileNet P8 help topic **System Administration** → **Enterprise-wide Administration** → **FileNet P8 Security** → **How to** → **Configure multiple realms**.

- a. Return to your completed Installation and Upgrade Worksheet file.

**Tip:** In the worksheet file, verify that the **Data** → **Filter** → **AutoFilter** command is enabled. To view only Enterprise Manager values for this task, filter by **EM: Create a Directory Configuration** in the **Installation or Configuration Program** column.

- b. In the FileNet P8 Logon dialog box, click **Connect**.
- c. In the Add Domain Configuration window, enter the values from your worksheet.
- d. In the Create P8 Domain window, enter the name for a new FileNet P8 domain from your worksheet and click **Continue** to start the Create a Directory Configuration wizard.

If an error occurs, check the application server log file on the machine where Content Engine is deployed.

Application server type	Path to log file
IBM WebSphere Application Server	<i>WAS_install_path/AppServer/profiles/profile_name/logs/server_name/SystemOut.log</i>
Oracle WebLogic Server	<i>WLS_install_path/user_projects/domains/domain_name/servers/server_name/logs/server_name.log</i>
JBoss Application Server	<i>JBOSS_DIST/server/server_name/log/server_name.log</i>

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

The Create a Directory Configuration wizard prompts you for many of the same parameters that you provided to Configuration Manager when you edited the Configure LDAP task.

See the topic for your directory service provider in the IBM FileNet P8 help topic **System Administration** → **Enterprise-wide Administration** → **FileNet P8 Security** → **Directory service providers**.

- f. In the Configure New Domain Permissions message box, click **OK** to acknowledge that the directory configuration is complete but remains in restricted mode. The Configure New Domain Permissions wizard automatically starts the first time you start Enterprise Manager if you have not defined any Global Configuration Data (GCD) administrators.
3. Configure permissions for the FileNet P8 domain.
  - a. Return to your completed Installation and Upgrade Worksheet file.

**Tip:** In the worksheet file, verify that the **Data** → **Filter** → **AutoFilter** command is enabled. To view only Enterprise Manager values for this task, filter by **EM: Configure New Domain Permissions** in the **Installation or Configuration Program** column.

- b. Complete the wizard screens by using the values in your worksheet.
  - c. In the Configure New Domain Permissions message box, click **OK**.
4. Close Enterprise Manager.

---

## Creating the data sources for an object store

Each object store in your site requires its own JDBC data sources. You can configure the data sources by using the Configuration Manager graphical user interface or the command line.

You created the JDBC data source for the Global Configuration Data (GCD) earlier in the configuration process. You must add the data sources now for at least one object store. You can create additional object store data sources as needed either immediately after you create the initial object store data sources or after you have confirmed your Content Engine configuration.

**Restriction:** Configuration Manager cannot create a data source that uses the same name as an existing data source. If you manually configured a data source by using your web application server administration tools, and you want to reuse the name, then you must manually delete the existing data source before you attempt to create the data source in Configuration Manager. See your web application server documentation for more information.

*“Creating the initial object store data sources by using the graphical user interface”*

You must create the JDBC data sources for each object store that Content Engine uses. Content 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 a single object store.

*“Creating additional object store data sources by using the graphical user interface” on page 73*

You must create the JDBC data sources for each object store that Content Engine uses. Content 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 a single object store, and you can add additional tasks as needed for each additional object store.

*“Creating the data sources by using the command line” on page 74*

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

## Creating the initial object store data sources by using the graphical user interface

You must create the JDBC data sources for each object store that Content Engine uses. Content 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 a single object store.

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 Configuration Manager, roll your mouse over the property name to view the hover help for the property.

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

Table 12. Required application server state

Option	Description
WebSphere Application Server	Start the application server if it is not already running.
JBoss Application Server	Stop the application server.
Oracle WebLogic Server	Start the application server 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. Select **File → 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 the task is enabled. 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 context 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 task execution status messages are displayed in the Console pane below the bootstrap properties.
10. (JBoss only) Start the application 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*.

## Related tasks

“Creating a new configuration profile” on page 26

Configuration Manager stores your settings for deploying a Content 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 Engine bootstrap settings, and the application deployment settings. You must create a new profile for each Content Engine instance that you are configuring.

“Configuration Manager user interface reference” on page 538

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content 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.

## Creating additional object store data sources by using the graphical user interface

You must create the JDBC data sources for each object store that Content Engine uses. Content 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 a single object store, and you can add additional tasks as needed for each additional object store.

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

The default configuration profile contains one task for configuring a single object store. You must create and run a new task for each additional object store in that Content Engine uses.

To configure the JDBC settings for additional object stores:

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 **CM: Configure JDBC data sources (object store 2)** in the **Installation or Configuration Program** column.

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


Table 13. Required application server state

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

3. If your configuration profile is not open in Configuration Manager, open it by select **File** → **Open** and navigating to your *profi lename .cfgp* file.

4. Create a task for the additional object store.
  - a. Right-click any *task name* in the profile pane, such as **Configure Object Store JDBC Data Sources**, and select **Add New Task** → **Configure JDBC Data Sources**. The **New\_Configure JDBC Data Sources** task is added to the profile.
  - b. Right-click **New\_Configure JDBC Data Sources**, and select **Rename Task**.
  - c. Enter a useful name for the task, such as **Configure Object Store 2 JDBC Data Sources**.
  - d. Click **OK**.
5. Right-click the **Configure Object Store 2 JDBC Data Sources** task in the profile pane, and select **Edit Selected Task**.
6. Provide the property values for the JDBC data sources for the object store by using the values in your worksheet for your additional object store.
7. Select **File** → **Save** to save your changes.
8. 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.
9. Ensure that the task is enabled. When the task is disabled, the task name includes the text **(disabled)**. To enable the task, right-click **Configure Object Store 2 JDBC Data Sources (disabled)** in the profile pane, and choose **Enable Selected Task** from the context menu.
10. Apply the JDBC property settings by right-clicking **Configure Object Store 2 JDBC Data Sources** 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.
11. (JBoss only) Start the application server.
12. Optional: Repeat this procedure as needed to add the data sources for each object store in your environment.

#### 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

“Configuration Manager user interface reference” on page 538

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content 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.

## Creating the data sources by using the command line

You must create the JDBC data sources for each object store that Content Engine uses. You must generate, edit, and execute a new `configurejdbc-os.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 `configurejdbc-os.xml` file for the initial object store data sources. If you have an existing `configurejdbc-os.xml` file, you can generate

another file for each additional object store. Each additional file that you add is named `configurejdbc-os.n.xml`. You can generate multiple `configurejdbc-os.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 `configurejdbc-os.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 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 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 `configurejdbc-os.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 ConfigureJDBC -profile myprofile
```
  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 3 on page 75 through 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*.

---

## Creating the initial object store

You create an initial object store in Content Engine to store your documents and other objects. After an object store is created, you can refine its definition and add content to it.

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

If you have not already done so, you must complete the following preparation tasks before you start the Create an Object Store wizard.

- Set up the initial storage area for the object store.
- Install the latest Content Engine service pack, as indicated in “Installing Content Engine software updates” on page 16.
- Create XA and non-XA data sources for the object store, as indicated in “Creating the data sources for an object store” on page 71).
- Read the FileNet P8 help topic *System Administration > Content Engine Administration > Object stores > Concepts*.

**Important:** The Create Object Store wizard fails to complete if you try to assign a new object store to a database or tablespace that is not completely empty.

To create 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 Enterprise Manager values for this task, filter by **EM: Create Object Store** in the **Installation or Configuration Program** column.

2. Start Enterprise Manager by double-clicking the Enterprise Manager desktop icon, or by choosing **Start** → **All Programs** → **FileNet P8 Platform** → **Enterprise Manager** .
3. In the FileNet P8 Logon screen, select the FileNet P8 domain in which you will create an object store, and then click **Connect**.
4. In the tree view, right-click the **Object Stores** container and choose **New Object Store** to start the Create an Object Store wizard.

**Important:** The maximum row size of the underlying DB2 database tables is 32 KB. Therefore, choose a minimal set of addons before creating an object store. After the object store exists, be aware that each user property reduces the row size from what already is reserved by the current system and addon properties. You should initially allocate string properties to be as small as possible; you can increase the sizes later in FileNet Enterprise Manager. A string property with a large allocation size is more space efficient if you create it as a long string data type; however, long strings have some functionality limitations.

5. 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*.

---

## Verifying the Content Engine installation

You can verify that the Content Engine installation succeeded by using IBM FileNet Enterprise Manager to create a folder and a document in each object store and then check the new document out and in.

To verify the Content Engine installation:

1. In Enterprise Manager, create a subfolder as follows:
  - a. Expand the **Object Stores container** and expand the node for the object store.
  - b. Right-click the **Root Folder icon**, and select **New Sub Folder**.
  - c. Enter a *folder name* and click **Create**.
  - d. Choose **Action** → **Refresh** to view the subfolder you created.
2. Create a document:
  - a. Expand the **Root Folder container**.
  - b. Right-click the *folder name* that you just created, and select **New Document**.
  - c. Enter the **Document Title** (for example, *Coffee Bean.bmp*), click **With content**, and click **Next**.
  - d. Click **Browse/Add** to select a file (for example, *C:\WINDOWS\Coffee Bean.bmp*), click **Open**, and then click **Create**. Notice that a new document

with a containment name matching the document title you used and a major version of 1 is now in your folder.

3. Check out a document as follows:
  - a. Right-click the document object that you just created (**Coffee Bean.bmp**), and select **Exclusive Check Out** (Default).
  - b. Navigate to the folder where you want the checked-out document to reside and click **Open**. Note the version number of the document.
  - c. Click **Yes** to edit the file.
  - d. Make some change to the file and save it.
  - e. Close the application you used to edit the file.
4. Check in the document:
  - a. Right-click the document object that you just edited (**Coffee Bean.bmp**), and select **Check In**.
  - b. In the **File Name** field, click **Browse/Add** .
  - c. Select the file that you checked out (**Coffee Bean.bmp**), and click **Open**.
  - d. Click **Check In**.
  - e. Right-click the **document object** that you just checked in, select **Properties**, and click the **Versions** tab of the Properties dialog box. Notice that the value of the Major Version field has been incremented.

---

## Installing and configuring Content Search Engine

This topic explains how to install and configure Content Search Engine.

“Installing Content Search Engine”

Use this procedure to install and configure IBM FileNet P8 Content Search Engine, an optional component based on the Autonomy K2 product.

“Configuring Content Search Engine” on page 88

Use this procedure to configure services required on the K2 Master Administration Server, and on additional Administration Servers you might install for IBM FileNet P8 Content Search Engine. All servers are configured through the Master Administration Server Dashboard.

“(optional) Installing additional locales” on page 93

You must install the locale files on all Autonomy K2 Administration Server machines only if you need more than basic content search locale functionality, for example, indexing and searching in languages other than English, Englishv, or basic UNI.

“Creating a Content Search Engine collections directory” on page 96

Use this procedure to configure the storage location and related security for your K2 collections.

“Configuring Content Engine for content-based retrieval” on page 98

You must use Enterprise Manager to configure an index area and enable the content-based retrieval (CBR) feature provided by the IBM FileNet P8 Content Search Engine.

“Verifying the Content Search Engine installation” on page 101

To verify that the Content Search Engine installation and configuration succeeded, perform the following procedure.

---

## Installing Content Search Engine

Use this procedure to install and configure IBM FileNet P8 Content Search Engine, an optional component based on the Autonomy K2 product.

“Overview” on page 80

Because Autonomy K2 software underlies Content Search Engine, you must install and configure Autonomy K2 on each machine in your Content Search Engine configuration.

“Installing Content Search Engine (UNIX)” on page 81

Install the Autonomy K2 software on each machine in your Content Search Engine configuration. You must complete a Master Administration software before you can add any additional K2 Administration Server installations. The Master Administration Server dashboard is the central control point for configuring Content Search Engine for single-server or multiserver installations.

“Installing Content Search Engine (Windows)” on page 85

Install the Autonomy K2 software on each machine in your Content Search Engine configuration. You must complete an installation of the Master Administration software before you can install additional K2 Administration Servers. The Master Administration Server dashboard is the central control point for configuring Content Search Engine for single-server or multiserver installations.

## Overview

Because Autonomy K2 software underlies Content Search Engine, you must install and configure Autonomy K2 on each machine in your Content Search Engine configuration.

The Autonomy K2 software is installed on each machine that is part of your Content Search Engine configuration. You must designate one machine in the configuration as the Master Administration Server. The Master Administration Server can be used as a stand-alone Content Search Engine; additional K2 Administration Servers can be added. All K2 Administration servers are configured and controlled through the K2 Dashboard of the Master Administration server.

The K2 software also includes K2 servers, K2 broker servers, K2 ticket servers, and K2 index servers. The K2 broker servers distribute search requests to the K2 servers, which perform the actual searches within the collections. Collections are the index files that contain pointers to indexed documents and the indexed words in those documents. The K2 index servers maintain the indexes. The K2 ticket servers implement document-level and collection-level security.

For information about additional Autonomy K2 functionality, see the Autonomy documentation that is installed with the Autonomy K2 Master Administration Server located at: `http://Master Administration Server hostname:9990/verity_docs/`. The Autonomy documentation set is not searchable from the IBM FileNet P8 Help but it does have its own internal index and search functionality.

### Important:

- Although the K2 Dashboard provides you with documentation for, and direct interfaces to, the K2 collections, IBM FileNet P8 requires that you use Enterprise Manager to manage collections associated with Content Search Engine index areas (for example, to add and remove index areas).
- Autonomy K2 was previously known as Verity, and you will see Verity still used in many of the interfaces described in the following procedures.
- If your Content Engine runs on Windows, then the machines in your Content Search Engine configuration must run on Windows. If your Content Engine runs on UNIX, then the machines in your Content Search Engine configuration must run on UNIX, but it doesn't have to be the same UNIX type.
- Where machine name variables are required, IP addresses will not validate. A valid name must be entered.
- If you unimport the style set, the original files will be deleted from your system. In this scenario, if you wish to re-import the style set, you must recover it from your installation package. In order to avoid this situation, you can either enter a unique name for the Style Set Alias during the initial Content Search Engine (Autonomy K2) installation, or make a backup copy of the original style set. If you enter a unique name for the style set during installation, ensure you use that name when you configure Content Engine for content-based retrieval.
- Stop word files can be used to increase performance by about 30%. You can place the `style.stp` file into the `stylefiles` directory to list words you do not want full-text indexed, for example, short words such as `a`, `the`, or `and`. However, any word in the stop word file cannot be searched. See the K2 documentation for more details. To create a stop word file you can typically copy the `vdk30.stp` file from either the main K2 install directory or the foreign language locales package over to the main `stylefile` directory, and then rename the file `style.stp`. You must do this copy operation before you create collections.

Because indexing is case sensitive, the `style.stp` file should include lower-case and upper-case versions of words in the stop word list. For example, use "the", "The" and "THE" if you think that all of these might be encountered in a search.

## Installing Content Search Engine (UNIX)

Install the Autonomy K2 software on each machine in your Content Search Engine configuration. You must complete a Master Administration software before you can add any additional K2 Administration Server installations. The Master Administration Server dashboard is the central control point for configuring Content Search Engine for single-server or multiserver installations.

The Master Administration Server's dashboard is the central control point for configuring all additional Administration Servers that are part of the Content Search Engine configuration.

You must designate each installation as either a Master Administration Server software installation or an Administration Server software installation.

**Important:** Only one K2 Master Administration Server can be installed for each Content Engine domain.

“Installing Content Search Engine interactively (UNIX)”

To install Content Search Engine interactively, you must run an installation program wizard.

“Installing Content Search Engine silently (UNIX)” on page 83

To install Content Search Engine silently, you must enter installations values into an input file and then run a command.

“Starting or stopping the Autonomy K2 services (UNIX)” on page 85

To manually start or stop the Autonomy K2 services on which Content Search Engine relies, you must use the commands provided by Autonomy.

### Installing Content Search Engine interactively (UNIX)

To install Content Search Engine interactively, you must run an installation program wizard.

To install Content Search Engine 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 Search Engine values, filter by **CSE Installer** in the **Installation or Configuration Program** column.

2. Log on to the host machine as `k2_os_user`.

**Important:** Most processes for the Autonomy K2 software will run as `k2_os_user`. However, the `vspget` process must run as root.

3. Set the following environment variable and place the entry in the `.profile` file for `k2_os_user`.

```
JAVA_HOME=java_(JDK)_install_path/jdkversion
export JAVA_HOME
```

4. Access the IBM FileNet P8 Content Search Engine installation package and run the installation program.

Platform	Command
AIX	P8CSE-4.5.1.0-AIX.BIN

Platform	Command
HPUX	P8CSE-4.5.1.0-HPUX.BIN
Solaris	P8CSE-4.5.1.0-SOL.BIN
Linux	P8CSE-4.5.1.0-LINUX.BIN

- Complete the installation program screens by using the values in your worksheet.
- Review the following Content Search Engine log files for installation errors. The files are located in the `verity` directory of the install path:

- `verity_install_path/cse_install_log_4_5_1.txt`
- `verity_install_path/vconfig.log`

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

- In the `.profile` file for `k2_os_user`, set the `PATH`, `SHLIB_PATH`, `LIBPATH`, and `LD_LIBRARY_PATH` environment variables (depending on your operating system), each on its own line, without line breaks.

**Important:** If your `.profile` file has a line containing `set -u` that appears before the lines involving `PATH`, `SHLIB_PATH`, `LIBPATH`, or `LD_LIBRARY_PATH`, you must do one of the following edits before setting the environment variables:

- Remove the line containing `set -u` from the `.profile` file.
- Move the line containing `set -u` to a point in the `.profile` file below the lines involving `PATH`, `SHLIB_PATH`, `LIBPATH`, or `LD_LIBRARY_PATH`.

#### AIX

```
PATH=$PATH:verity_install_path/k2/_rs6k43/bin
export PATH
LIBPATH=$LIBPATH:verity_install_path/k2/_rs6k43/bin
export LIBPATH
```

#### HP-UX

```
PATH=$PATH:verity_install_path/k2/_hpux/bin
export PATH
SHLIB_PATH=$SHLIB_PATH:verity_install_path/k2/_hpux/bin
export SHLIB_PATH
```

#### Linux

```
PATH=$PATH:verity_install_path/k2/_ilnx21/bin
export PATH
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:verity_install_path/k2/_ilnx21/bin
export LD_LIBRARY_PATH
```

#### Solaris

```
PATH=$PATH:verity_install_path/k2/_sso126/bin
export PATH
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:verity_install_path/k2/_sso126/bin
export LD_LIBRARY_PATH
```


- Access the host machine and log on as a user with root privileges.
- Enter the following commands to set the `setuid` bit for the `vspget` program so that the service runs as root:

```
chown root verity_install_path/k2/_platform/bin/vspget
chmod u+s verity_install_path/k2/_platform/bin/vspget
```

Replace `_platform` with the following directory:

Platform	Directory
AIX	_rs6k43
HPUX	_hpux
Solaris	_ssol26
Linux	_ilnx21

### 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 Content Search Engine silently (UNIX)

To install Content Search Engine silently, you must enter installations values into an input file and then run a command.

To install Content Search Engine silently on UNIX:

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 Search Engine values, filter by **CSE Installer** in the **Installation or Configuration Program** column.

2. Log on to the host machine as *k2\_os\_user*.

**Important:** Most processes for the Autonomy K2 software will run as *k2\_os\_user*. However, the *vspget* process must run as root.

3. Set the following environment variable and place the entry in the *.profile* file for *k2\_os\_user*.

```
JAVA_HOME=java_(JDK)_install_path/jdkversion
export JAVA_HOME
```

4. Access the IBM FileNet P8 Content Search Engine installation package.
5. Edit the *cse\_silent\_install.txt* file to reflect the appropriate responses for your installation by using the values from your worksheet.
6. Run the IBM FileNet P8 Content Search Engine installation program by executing one of the following commands:

Platform	Command
HPUX	P8CSE-4.5.1.0-HPUX.BIN -f CSE_silent_install.txt -i silent
AIX	P8CSE-4.5.1.0-AIX.BIN -f CSE_silent_install.txt -i silent
Solaris	P8CSE-4.5.1.0-SOL.BIN -f CSE_silent_install.txt -i silent
Linux	P8CSE-4.5.1.0-LINUX.BIN -f CSE_silent_install.txt -i silent

7. Review the following Content Search Engine log files for installation errors. The files are located in the *verity* directory of the install path:

- *verity\_install\_path/cse\_install\_log\_4\_5\_1.txt*
- *verity\_install\_path/vconfig.log*

It is a best practice to review log files even if the Content Search Engine installation program does not indicate any errors. Some errors noted in the log



files are benign. If an error is not benign (that is, you cannot subsequently index or search for documents), refer to the log file for help in determining the cause.

8. In the `.profile` file for `k2_os_user`, set the `PATH`, `SHLIB_PATH`, `LIBPATH`, and `LD_LIBRARY_PATH` environment variables (depending on your operating system), each on its own line, without line breaks.

**Important:** If your `.profile` file has a line containing `set -u` that appears before the lines involving `PATH`, `SHLIB_PATH`, `LIBPATH`, or `LD_LIBRARY_PATH`, you must do one of the following edits before setting the environment variables:

- Remove the line containing `set -u` from the `.profile` file.
- Move the line containing `set -u` to a point in the `.profile` file below the lines involving `PATH`, `SHLIB_PATH`, `LIBPATH`, or `LD_LIBRARY_PATH`.

#### AIX

```
PATH=$PATH:verity_install_path/k2/_rs6k43/bin
export PATH
LIBPATH=$LIBPATH:verity_install_path/k2/_rs6k43/bin
export LIBPATH
```

#### HP-UX

```
PATH=$PATH:verity_install_path/k2/_hpux/bin
export PATH
SHLIB_PATH=$SHLIB_PATH:verity_install_path/k2/_hpux/bin
export SHLIB_PATH
```

#### Linux

```
PATH=$PATH:verity_install_path/k2/_ilnx21/bin
export PATH
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:verity_install_path/k2/_ilnx21/bin
export LD_LIBRARY_PATH
```

#### Solaris

```
PATH=$PATH:verity_install_path/k2/_ssol26/bin
export PATH
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:verity_install_path/k2/_ssol26/bin
export LD_LIBRARY_PATH
```


9. Access the host machine and log on as a user with root privileges.
10. Enter the following commands to set the `setuid` bit for the `vspget` program so that the service runs as root:

```
chown root verity_install_path/k2/_platform/bin/vspget
chmod u+s verity_install_path/k2/_platform/bin/vspget
```

Replace `_platform` with the following directory:

Platform	Directory
AIX	_rs6k43
HPUX	_hpux
Solaris	_ssol26
Linux	_ilnx21

## 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*.


## Starting or stopping the Autonomy K2 services (UNIX)

To manually start or stop the Autonomy K2 services on which Content Search Engine relies, you must use the commands provided by Autonomy.

1. Log on as the user `k2_os_user` at the machine where Autonomy K2 services are installed
2. Run one of the following commands, depending on the operating system:

Option	Description
HP-UX	Start services: <code>nohup verity_install_path/k2/_hpux/bin/k2adminstart &amp;</code>  Stop services: <code>verity_install_path/k2/_hpux/bin/k2adminstop</code>
AIX	Start services: <code>nohup verity_install_path/k2/_rs6k43/bin/k2adminstart &amp;</code>  Stop services: <code>verity_install_path/k2/_rs6k43/bin/k2adminstop</code>
Solaris	Start services: <code>nohup verity_install_path/k2/_ssol26/bin/k2adminstart &amp;</code>  Stop services: <code>verity_install_path/k2/_ssol26/bin/k2adminstop</code>
Linux	Start services: <code>nohup verity_install_path/k2/_ilnx21/bin/k2adminstart &amp;</code>  Stop services: <code>verity_install_path/k2/_ilnx21/bin/k2adminstop</code>

## 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 Content Search Engine (Windows)

Install the Autonomy K2 software on each machine in your Content Search Engine configuration. You must complete an installation of the Master Administration software before you can install additional K2 Administration Servers. The Master Administration Server dashboard is the central control point for configuring Content Search Engine for single-server or multiserver installations.

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

The Master Administration Server dashboard is also the central control point for configuring all additional Administration Servers that are part of the Content Search Engine configuration.

You must designate each installation as either a Master Administration Server software installation or an Administration Server software installation.

**Important:** Only one K2 Master Administration Server can be installed for each Content Engine domain.

You can install Autonomy K2 software either interactively or silently.

“Installing Content Search Engine interactively (Windows)”

To install Content Search Engine interactively, you run a program wizard.


“Installing Content Search Engine silently (Windows)” on page 87

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

“Setting the logon user for the K2 Administration Server service (Windows)” on page 87

To avoid problems when indexing documents using UNC, or viewing UNC-indexed documents, the *k2\_os\_user* needs to run the K2 Administration Server service.

### 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 Content Search Engine interactively (Windows)

To install Content Search Engine interactively, you run a program wizard.

To install Content Search Engine 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 Search Engine values, filter by **CSE Installer** in the **Installation or Configuration Program** column.


2. Log on to the host machine as *k2\_os\_user*.
3. Access the IBM FileNet P8 Content Search Engine installation package and run the P8CSE-4.5.1.0-WIN.EXE file.
4. Complete the installation program screens by using the values in your worksheet.
5. Review the following Content Search Engine log files for installation errors. The files are located in the *verity* directory of the installation path:
  - *verity\_install\_path*\cse\_install\_log\_4\_5\_1.txt
  - *verity\_install\_path*\vconfig.log

It is a best practice to review log files even if the Content Search Engine installation program does not indicate any errors. Some errors noted in the log

files are benign. If an error is not benign (that is, you cannot subsequently index or search for documents), refer to the log file for help in determining the cause.

6. After the installation finishes, complete the following substeps:
  - a. Verify that the Verity K2 Administration Web Server service (Tomcat server) is installed and has started.
  - b. Verify that the Verity K2 6.2.1 Administration Server service exists.

#### 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 Content Search Engine silently (Windows)

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

To install Content Search Engine 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 Search Engine values, filter by **CSE Installer** in the **Installation or Configuration Program** column.

2. Log on to the host machine as *k2\_os\_user*.
3. Edit the `cse_silent_install.txt` file to reflect the appropriate responses for your installation by using the values from your worksheet.
4. Run the IBM FileNet P8 Content Search Engine installation program by executing the following command:

```
P8CSE-4.5.1.0-WIN.EXE -f CSE_silent_install.txt -i silent
```
5. Review the following Content Search Engine log files for installation errors. The files are located in the `verity` directory of the installation path:
  - `verity_install_path\cse_install_log_4_5_1.txt`
  - `verity_install_path\vconfig.log`

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

#### 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*.

### Setting the logon user for the K2 Administration Server service (Windows)

To avoid problems when indexing documents using UNC, or viewing UNC-indexed documents, the *k2\_os\_user* needs to run the K2 Administration Server service.

To set the logon user for the K2 Administration Server service:

1. Open the Windows Services window (for example, on Windows Server 2003, right-click My Computer and choose **Manage** → **Services and Applications** → **Services** select Manage Services and Applications | Services).
2. Select and double-click the Verity K2 6.1 Administration Server service.
3. Click the **Log On** tab, enter the *k2\_os\_user* user and password under which Autonomy K2 services will run, and click **OK**.

**Important:** Whenever you change the password for the *k2\_os\_user* account, you must update the password on this tab as well. Otherwise, the K2 Administration Server will not start when you restart the machine. Also, depending on your domain controller group policy settings, the password for this account may be reset, which will result in logon failures for the K2 Administration Server service when the machine is restarted. To avoid these failures, contact your Windows administrator.

4. Restart the Verity K2 6.1 Administration Server service.

---

## Configuring Content Search Engine

Use this procedure to configure services required on the K2 Master Administration Server, and on additional Administration Servers you might install for IBM FileNet P8 Content Search Engine. All servers are configured through the Master Administration Server Dashboard.

- When you name the servers that you create, it is a best practice to indicate the type of server in the server name. Otherwise, when you configure Content Engine by using Enterprise Manager, it can be difficult to determine which server to select for an action. For example, use *server\_name\_broker* to indicate a Broker Server service.
- Record the server names, port numbers, and settings that you define. Much of the following information will be required later when you configure the IBM FileNet P8 Content Engine for content-based retrieval later.
- A range of ports is recommended in the Verity K2 Dashboard for each service you create. You do not have to choose a port number from within that range.
- Repeat the related step in the procedure below to add additional services. Some guidelines must be adhered to when adding additional services:
  - Multiple brokers can be assigned, so that if one goes down the others will be used. However, each broker must have all K2 Servers (search servers) attached that are needed to access collections (index areas). The Content Engine Server will not call multiple brokers and merge the results.
  - If you add additional Index Servers and K2 Servers (search servers), they will not be activated until you enable them through Enterprise Manager. See Configure Content Engine for content-based retrieval for details.
  - Each K2 Administration Server must contain a Ticket Server for Content Engine.
  - For good stability and performance, Broker Servers must be attached to local Ticket Servers for security on each machine.
- In the following procedure you must import the IBM FileNet Styleset only once, regardless how many K2 Administration Server machines you install.

To configure Content Search Engine:

1. (Optional) Configure the Autonomy K2 Dashboard to use SSL security. The Autonomy K2 Dashboard web application, by default, uses a non-SSL web site

and sends username and password information in plain text. For information on how to modify your Tomcat web applications to use SSL, access the following address:

<http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html>

2. Access the K2 Dashboard by launching your browser and entering:  
[http://Master Administration Server hostname:9990/verity\\_dashboard/main.jsp](http://Master Administration Server hostname:9990/verity_dashboard/main.jsp)
3. Create a K2 Index Server, as follows:
  - a. Click **K2 Index Servers** under **System View**.
  - b. Click **Add a K2 Index Server** on the K2 Index Server Summary page.
  - c. Enter the following information on the Configure basic settings for the new K2 Index Server page:
    - Service Alias: *server\_name\_index\_server*
    - Port: 9960 - 9979 (suggested range)
  - d. Click **Next** to continue with the installation.
  - e. Enter the following information on the Configure threads for the K2 Index Server page:
    - Synchronous Threads: 25
    - Asynchronous Threads: 3
    - Access Type: *Authorized Administrator*
  - f. Click **Finish** to continue with the installation.
4. Set the Index Server logging properties:
  - a. Click the Index Server, under System View, that you want to adjust.
  - b. Click **Edit Properties** under Actions.
  - c. Click the **Logging** tab.
  - d. For Status Log Nominal Size, enter the following value:  
9000 kilobytes
  - e. Click **Modify**.
5. Create a K2 Broker Server:
  - a. Click **K2 Brokers** under **System View**.
  - b. Click **Add a K2 Broker** on the K2 Broker Summary page.
  - c. Enter the following information on the Configure basic settings for the new K2 Broker page:
    - Service Alias: *server\_name\_broker*
    - Port: 9900 - 9909 (suggested range)
  - d. Click **Finish**.
6. Create a K2 Server (search server) and attach the Broker:
  - a. Click **K2 Servers** under **System View**.
  - b. Click **Add a K2 Server** under **Actions** on the K2 Server Summary page.
  - c. Enter the following information on the Configure basic settings for the new K2 Server page:
    - Service Alias: *server\_name\_search\_server*
    - Port: 9920 - 9949 (suggested range)
  - d. Click **Next**.
  - e. Click **Next** on the Set security options for this service page.
  - f. Enter the following information on the Attach to K2 Brokers page:

- Select the K2 Brokers that will provide access to this service: Select the K2 Broker you created in step 3 from the drop-down menu, *server\_name* \_broker.
- g. Click **Finish**.
7. Import the IBM FileNet Styleset.
- a. Click **Collections** under System View.
  - b. Click **Manage Style Sets** under **Actions** on the Collection Summary page.
  - c. Click **Import** on the Manage Style Sets page (top right).
  - d. Enter the following information on the Import page:
    - Style Set Alias: *FileNet\_FileSystem\_PushAPI*
    - Gateway Type: --Auto-detect--
    - Source Administration Server. If multiple servers are installed, choose the server to which you will import the Styleset.
    - Source Path:

**Windows**

```
verity_install_path\data\stylesets\
FileNet_FileSystem_PushAPI
```

**UNIX** *verity\_install\_path/data/stylesets/  
FileNet\_FileSystem\_PushAPI*

- e. Click **Import**.

**Tip:** The K2 Dashboard displays a notification that the StyleSet Editor web application cannot be accessed. You can ignore this message because it relates to a function that is not used by IBM FileNet P8 Content Search Engine.

8. Navigate to the source path you specified in the preceding step and complete the following substeps:
- a. Open the file *style.ufl* for editing.
  - b. If it is not already present, add the CEMP definition at the bottom of the file:
 

```
data-table: fce
{
 fixwidth: cemp_partition_date 4 unsigned-integer
}
```
  - c. Save and close the file.
9. Create a K2 Ticket Server.
- a. Click **K2 Ticket Servers** under **System View**.
  - b. Click **Add a K2 Ticket Server** under **Actions** on the **K2 Ticket Server Summary** page.
  - c. Enter the following information on the Configure basic settings for the new K2 Ticket Server page:
    - Service Alias: *server\_name* \_ticket\_server
    - Port: 9910 - 9919 (recommended range)
  - d. Click **Next**.
  - e. Enter the following information on the Configure the login module to use with this K2 Ticket Server page:
    - Select which Login Module type to use with this K2 Ticket Server:
      - Windows
      - UNIX



- Restriction:** LDAP Ticket Servers are not currently supported.
- Default Domain (Windows only): Enter the domain on which this user and K2 Server are authenticated. If the server is in a workgroup, leave this field blank.
- f. Click **Next**.
  - g. Enter the following information on the Configure the persistent store module to use with this K2 Ticket Server page:
    - Select the Persistent Store Module type to use with this K2 Ticket Server: Choose File and Memory.
  - h. Click **Finish**.
  - i. (Windows only) Specify local login settings:
    - 1) Click **Edit Properties**.
    - 2) Click Windows Login Module.
    - 3) Check **Use Local Credentials**.
    - 4) Check Enable Built-in Groups.
    - 5) Click **Modify**.
10. Set Autonomy K2 Administration Security.
- a. Click the K2 Ticket Server you created.
  - b. Click **Manage Administration Security** under Actions.
  - c. Enter the following information on the **Manage Administration Security** page:
    - Select a K2 Ticket Server to configure for administration security: From the drop-down menu, select the K2 Ticket Server you just created.
    - User Name: Enter the k2\_os\_user. For UNIX installs, this is the user you logged in as to run the installation.
    - Password: Enter the authentication password.
    - Default Domain (Windows only): Enter the domain on which this user and K2 Server are authenticated. If the server is in a workgroup, leave this field blank.
  - d. Click **Modify**.
 

The K2 software will authenticate the user based on the information you entered. If the check fails, an error message will indicate what failed and request that you re-enter the information.

If administrator access is successful, Autonomy K2 will close the Dashboard and require that you log on again as the Dashboard Administrator to complete the configuration.
11. Launch the K2 Dashboard and log on.
12. Restart K2 services:
- a. Under **Notifications** on the K2 Dashboard Home page, a number of servers are listed as requiring a restart. Click **Start/Stop this Service** to access the settings page and follow the instructions listed there. Choose **Full Restart** to ensure that all services start as expected.
  - b. Click **Home** in the top-left corner of the page after each restart to view the remaining notifications. Repeat the process until there are no notifications remaining.
13. Enable additional K2 Admin Users (optional).
- a. From the K2 Dashboard home page, click **Administration Servers**.
  - b. Click **Manage K2 Administrative Users**.

- c. Click **Add User** on the **Manage K2 Administrative Users** page.
  - d. Enter the name of an authenticated user on the directory service that you want to make a K2 Administrator and click **Add**.
14. Enable security on the K2 services you have created.
- a. From the K2 Dashboard home page, click **K2 Ticket Servers**.
  - b. Click your ticket server *server\_name\_ticket\_server*.
  - c. Click **Manage K2 Broker/K2 Server Security** in the Services Secured by this K2 Ticket Server section of the page (bottom right).
  - d. Click the **K2 Servers** button on the **Manage K2 Broker/K2 Server Security** page.
  - e. Click the service you just created which is listed in the window on the right to enable security.

**Important:** If you have a multi-server configuration, numerous services, installed on other machines, will be listed also. Select only the service to which you want to attach a broker. Brokers must be attached to local ticket servers for Content Search Engine.

- f. Click the **K2 Brokers** button on the **Manage K2 Broker/K2 Server Security** page.
  - g. Click the Broker in the window on the right that you want to attach to the local K2 ticket server you selected above.
  - h. Click **Modify** to save your changes.
15. Restart K2 services, as follows:
- a. Click **Home** in the top left corner of the page.
  - b. Under **Notifications** on the Verity K2 Dashboard Home page, a number of servers are listed as requiring a restart. Click **Start/Stop this Service** to access the settings page and follow the instructions listed there. Choose **Full Restart** to ensure that all services start as expected. Click **Home** in the top left corner of the page after each restart to view the remaining notifications. Repeat the process until there are no notifications remaining.

#### “Configuring services on Administration Servers”

Use this procedure to create and configure services on specific Content Search Engine machines (Administration Servers), other than the Master Administration Server. Services for all machines in your Content Search Engine configuration are configured through the Master Administration Server Dashboard.

#### Related concepts

 Specifying accounts

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

## Configuring services on Administration Servers

Use this procedure to create and configure services on specific Content Search Engine machines (Administration Servers), other than the Master Administration Server. Services for all machines in your Content Search Engine configuration are configured through the Master Administration Server Dashboard.

1. Click **Administration Servers** under **System View**.
2. Click the Administration Server to which you want to add services.
3. Click **Add a Service** under K2 Services on this Administration Server.
4. Select the service you want to add.

5. Follow the instructions and guidelines for the appropriate service in the To configure Content Search Engine procedure above to complete the service addition.

---

## (optional) Installing additional locales

You must install the locale files on all Autonomy K2 Administration Server machines only if you need more than basic content search locale functionality, for example, indexing and searching in languages other than English, Englishv, or basic UNI.

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

You need to know *k2\_os\_user* (the user who installed Content Search Engine), and *verity\_install\_path* (the installation path of Autonomy K2) from your installation of Content Search Engine.

### **Important:**

- A Locales installer screen indicates that the installer is compatible only with Autonomy K2 version 6.2.0. However, the Locales installer is compatible with version 6.2.1, the version you installed with IBM FileNet P8 Content Search Engine 4.5.
- When the Locales installer prompts you for your installed version of Autonomy K2 from a dropdown menu, select K2 6.2.0.

**Important:** Although the Locales installer offers the option of installing to a location other than the Verity install location, do not choose this option. For Content Search Engine, you must install the locales to the k2 directory of the Autonomy K2 installation path.

1. Open your completed Installation and Upgrade worksheet.

**Tip:** In the worksheet file, verify that the **Data → Filter → AutoFilter** command is enabled. To view only Locales installer values, filter by **CSE: Verity Locales 6.2.0 Installer** in the **Installation or Configuration Program** column.

2. Run the Locales installation, depending on your operating system.  
“Installing additional locales (UNIX)”  
Install non-English locales on UNIX machines only if you need them.  
“Installing additional locales (Windows)” on page 95  
Install non-English locales on Windows machines only if you need them.

## Installing additional locales (UNIX)

Install non-English locales on UNIX machines only if you need them.

1. Access the Autonomy K2 Master Administration Server machine and log on as *k2\_os\_user*.
2. Copy the Locales installation package, P8CSE-4.5.1.0-Locales.zip, for your platform from the installation package to the machine and extract its contents to a local directory.
3. Run the following command (with no line break) to stop the Autonomy K2 services.

Operating System	Command
AIX	<code>verity_install_path/k2/_rs6k43/bin/k2adminstop</code>
HP-UX	<code>verity_install_path/k2/_hpux/bin/k2adminstop</code>
Linux	<code>verity_install_path/k2/_ilnx21/bin/k2adminstop</code>
Solaris	<code>/verity_install_path/k2/_ssol26/bin/k2adminstop</code>

4. Add the following lines to the `.profile` file of `k2_os_user`:  

```
VERITY_CFG=verity_install_path/k2/common/verity.cfg
export VERITY_CFG
```
5. Navigate to the directory where you extracted the Locales installation package and run one of the following installation programs:

Platform	Command
AIX	<code>setupaix.bin</code>
HPUX	<code>sethpux.bin</code>
Linux	<code>setLinux.bin</code>
Solaris	<code>setSolaris.bin</code>

**Important:** If the installer prompts you to choose whether to replace existing files that are newer than the files to be installed, click **No to All**

6. When prompted, select the **Install all platform binaries** option if you want licensed language locales for the UNIX operating system where you are installing Locales, but also for Windows and the other supported UNIX operating systems.
7. When prompted, specify the following license key: 2UV4MPT-2KPEQBJ-1D6A6KT-2KPE6KT-2KPE6KS.
8. When the installation program finishes, run the following command:  

```
chmod -R 777 verity_install_path/k2/common/basdata
```
9. Run the following command to check the parameter that controls the maximum file size:  

```
ulimit -f
```
10. If the maximum file size is not unlimited, complete the following substeps:
  - a. Set the value of the `default:fsize` line in the file `/etc/security/limits/` file as follows and save your edit.  

```
default:fsize=-1
```
  - b. Log off the machine and log back on as `k2_os_user`.
11. Navigate to the local directory to which you extracted the Locales installation package and extract the contents of `cse-451.locales.supplement.tar.gz`, which creates a subdirectory `k2`.
12. Run the following command on the `k2` directory:  

```
chmod -R 777 k2
```
13. Copy the extracted directory `k2` into the `verity_install_path` directory. For example, if `verity_install_path` is `/opt/IBM/FileNet/ContentEngine/verity`, run the following command:  

```
cp -r k2 /opt/IBM/FileNet/ContentEngine/verity
```

14. Start the Verity K2 services, as follows:

Operating System	Command
AIX	<code>nohup verity_install_path/k2/_rs6k43/bin/k2adminstart</code>
HP-UX	<code>nohup verity_install_path/k2/_hpux/bin/k2adminstart</code>
Linux	<code>nohup verity_install_path/k2/_ilnx21/bin/k2adminstart</code>
Solaris	<code>nohup verity_install_path/k2/_ssol26/bin/k2adminstart</code>

15. Run the following command to ensure that the locale license information is synchronized with the Master Administration Server:

```
rcadmin -update
```

## Installing additional locales (Windows)

Install non-English locales on Windows machines only if you need them.

1. Access the Autonomy K2 Master Administration Server machine and log on as *k2\_os\_user*.
2. Copy the Locales installation package, P8CSE-4.5.1.0-Locales.zip for your platform from the installation package to the machine and extract its contents to a local directory.
3. Stop the Autonomy K2 services, as follows:
  - a. Access Component Services.
  - b. Stop the Verity K2 Administration Server service and the Verity K2 Administration Web Server service.
4. Navigate to the decompressed Locales installer location and run the following command to start the Locales installer:

```
setupwin32.exe
```
5. At the Welcome screen, click **Cancel**, and then click **Yes** to exit.

**Important:** By opening the Welcome screen, the Locales installer creates the *\_vpddb* directory (and parent directories), which will contain the *vpd.script* file. This file contains a parameter that allows the Locales installer to find the existing Autonomy K2 installation. The path to the *\_vpddb* directory has the following form:

```
32 bit: C:\Program Files\Common Files\InstallShield\Universal\WinVersion\
x86\host_name\Gen1_vpddb
```

```
64-bit: C:\Program Files (x86)\Common Files\InstallShield\Universal\
WinVersion\x64\host_name\Gen1_vpddb
```

where *WinVersion* is the name of the Windows operating system, and *host\_name* is the name of the K2 Master Administration Server machine.

6. Locate the *vpd.script* file in *verity\_install\_path*, open the file in a text editor, and make the following edits:
  - Replace the instance of `<K2InstallDir>` with your *verity\_install\_path*. For example: `C:\Program Files\IBM\FileNet\ContentEngine\verity`.
  - Replace both instances of `<myHostName>` with the Master Administration Server machine name.

- Replace both instances of <WinVersion> with the value of *WinVersion* that the Locales installer generated in 5 on page 95.
7. Copy the `vpd.script` file that you edited in 6 on page 95 to the `_vpddb` directory that the Locales installer created in 5 on page 95, overwriting the existing `vpd.script` file in that location.
  8. Navigate to the decompressed Locales installer location and run the following command to start the Locales installer. The installer will locate the K2 installation based on the settings you specified in 6 on page 95.  
`setupwin32.exe`
- Important:** If the installer prompts you to choose whether to overwrite files that are newer than those to be installed, click **No to All**.
9. When prompted, select the **Install all platform binaries** option if you want licensed language locales not only for the Windows operating system on the machine where you are installing Locales, but also for all the supported UNIX operating systems.
  10. When prompted, specify the following license key: 2UV4MPT-2KPEQBJ-1D6A6KT-2KPE6KT-2KPE6KS.
  11. When the Locales installer completes, install the Locales supplement, as follows:
    - a. Copy the Locales supplement file `P8CSE-4.5.0-002-LOCALESSUPPLEMENT.zip` from the installation media and extract it into a temporary directory on the machine where you installed Locales. Extracting the Locales supplement creates a subdirectory named `k2` in the temporary directory.
    - b. Copy the `k2` subdirectory and paste it into `verity_install_path` directory. Overwrite any existing files that have the same name as those in `k2`.
  12. Start the Autonomy K2 services that you stopped in 3 on page 95.
  13. Run the following command to ensure that the locale license information is synchronized with the Master Administration Server:  
`rcadmin -update`

---

## Creating a Content Search Engine collections directory

Use this procedure to configure the storage location and related security for your K2 collections.

“Collections directory requirements”

The task of creating a collections directory includes setting up security permissions to allow read and write access.

### Collections directory requirements

The task of creating a collections directory includes setting up security permissions to allow read and write access.

**Important:** Contrary to information outlined in the Autonomy-supplied documentation set, remote collections are not supported for use with IBM FileNet P8 Content Search Engine. Collections must be written locally to the Autonomy K2 server. Using a remote-mounted disk that is accessed via the network (NFS, PCNFS, or CIFS) will cause stability problems under load and corrupt your collections. Any existing configurations that contain non-local collections directories must be re-configured.

For performance reasons, create one collections directory for each index area that you create in IBM FileNet P8 Content Engine. Each collections directory you create must be set to provide proper security access as outlined below. The path to both the collections directory and collections temp directory must be entered in the index area properties when you create the index area.

Security and communication between Autonomy K2 Content Engine, and the collections directory is handled through the user accounts and permissions provided to those accounts.

For detailed information on security, see the IBM FileNet P8 help topic **System Administration** → **Enterprise-wide Administration** → **FileNet P8 Security** → **Authorization** → **Security for integrated components and third-party products** → **Autonomy K2 Server** → **Security for Autonomy K2 Server**.

To create a collections directory:

1. On the Autonomy K2 server, create a directory in which you will store K2 collections. Give read, write, and execute permissions to the *k2\_os\_user*.  
This path must be local to the index server that will be assigned to write collections. This is the same index server that you created when you configured Content Search Engine.
2. Create a temp directory on the Autonomy K2 machine on which you created the collections directory. The temp directory will be used by the K2 Index Server and Content Engine Server during operations.  
This path must be visible to both the Content Engine and the Content Search Engine servers. If the K2 Master Administration Server and Content Engine are not installed on the same machine, they both must be on a network-mounted file system.
3. Record the collections directory path in the Autonomy K2 configuration file.

Option	Description
<b>Windows</b>	<ol style="list-style-type: none"> <li>1. Open the following K2 configuration file in a text editor: <i>verity_install_path</i>\k2\common\<i>verity.cfg</i></li> <li>2. Modify the next available alias settings by adding the collections path, where new collections will be written. For example, change <i>alias6</i>, <i>mapping6</i>, and <i>dirmode6</i> to the following: <i>alias6=path1</i> <i>mapping6=C:\Collections_Directory</i> <i>dirmode6=wr</i></li> <li>3. Save our edits.</li> </ol>



Option	Description
UNIX	<ol style="list-style-type: none"> <li>1. Open the following K2 configuration file in a text editor: <code>verity_install_path/k2/common/verity.cfg</code></li> <li>2. Modify the next available alias settings by adding the collections path. For example, change <code>alias6</code>, <code>mapping6</code>, and <code>dirmode6</code> to the following: <code>alias6=path1</code> <code>mapping6=/Collections_Directory_Path</code> <code>dirmode6=wr</code>  <b>Note:</b> The <code>Collections_Directory_Path</code> must be a local path and not a mount point.</li> <li>3. Save your edits.</li> </ol>

### Related concepts

 Specifying accounts

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

---

## Configuring Content Engine for content-based retrieval

You must use Enterprise Manager to configure an index area and enable the content-based retrieval (CBR) feature provided by the IBM FileNet P8 Content Search Engine.

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

Take the following issues into account before you configure Content Engine.

- Various server names and related ports assigned during the installation and configuration of Autonomy K2 are required during this procedure. For a record of the servers created and the ports that have been assigned, log on to the Autonomy K2 dashboard.
- If you unimport the style set, the original files are deleted from your system. In this scenario, if you want to reimport the style set, you must recover it from your installation disk.
- Where machine name variables are required, IP addresses cannot be specified. In these cases, you must enter the host name for the machine.

For more detail on content-based retrieval and Content Engine, see the IBM FileNet P8 help topic **System Administration** → **Content Engine Administration** → **Content-based retrieval** → **How to...** → **Configure CBR**.

To configure Content Engine for content-based retrieval:

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 Enterprise Manager values for this task, filter by **EM: Verity Domain Configuration Tab** in the **Installation or Configuration Program** column.

2. Start Enterprise Manager and log on as the GCD Administrator.
3. Create a Verity Domain Configuration (VDC).
  - a. Right-click **Enterprise Manager [domain]** in the Enterprise Manager tree and select **Properties**.
  - b. Click the **Verity Domain Configuration** tab.
  - c. Enter the following K2 Master Administration Server access information:
    - Host Name - the name of the host of the K2 Master Administration Server.
    - Port - the K2 Master Administration Server port. The default port number is 9950.
    - User Domain - the authentication domain in which your K2 services are installed.
    - User Group - K2 Security Group.
    - Verity Username - K2 Security User.
    - Password - the K2 Security User password.
  - d. Click **Create Configuration** to create a Verity Domain Configuration object.
4. Assign a K2 Broker Server:
  - a. Click the **Verity Server** tab.
  - b. From the Brokers AVAILABLE pane, select the broker and click **Add** to move the server to the Brokers Selected pane.
  - c. Click **OK**.

**Important:** You can assign multiple Broker Servers to a K2 Administration Server, primarily for failover. If one Broker Server goes down, then K2 can switch to another. In this configuration, you must ensure that all Search Servers required to access K2 Collections (index areas) are attached to each Broker Server. A given Content Engine server does not call multiple Broker Servers or merge associated search results. See the appropriate steps of the Configure Content Search Engine task for instructions on how to create Broker Servers and assign Search Servers.

5. To assign a CBR locale to the object store for which you want to enable indexing, complete the following substeps:
  - a. Right-click the object store in the left pane of Enterprise Manager and choose **Properties** from the context menu.
  - b. In the Properties dialog box, click the **CBR** tab.
  - c. Specify one of the following locales (which are installed by default with Autonomy K2 Content Search Engine software) in the CBR Locale box:
    - uni (multi-language and slower indexing)
    - englishv (enhanced word-stemming and faster indexing)
    - english (limited capabilities and fast indexing)

If you click **Set to Default CBR Locale**, the CBR locale is set to *uni*.
  - d. Click **Apply** or **OK**.
6. To access the Verity Locale Configuration Guide, complete the following substeps.

**Important:** For information about how the K2 product uses locales and about performance and indexing options, review the Verity Locale Configuration Guide in the Autonomy-supplied documentation set.

- a. Open the Autonomy K2 Dashboard and click **Help**.
  - b. Click **Library** (top right of the screen) to access the Autonomy K2 product guides. Each guide is available in HTML or PDF format.
7. Create an index area.
- a. 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 Enterprise Manager values for this task, filter by **EM: Create an Index Area** in the **Installation or Configuration Program** column.

- b. In the Enterprise Manager tree view, expand the **Object Stores** container.
  - c. Right-click the object store to which you want to add an index area and select **New** → **Index Area**.
  - d. Complete the Create an Index Area wizard by using the values from your worksheet.
- For more information about creating indexes, see the IBM FileNet P8 help topic **System Administration** → **Content Engine Administration** → **Content-based retrieval** → **How to...** → **Create Verity index area**.
8. Enable CBR for one or more document class definitions:
- a. Right-click the class you want to configure, such as a document class that your site has created, in the Enterprise Manager tree and click **Properties**.
  - b. Select the **CBR Enabled** check box and click **OK**.
9. Enable CBR for one or more string properties of the document classes or custom object classes that you want to use for content-based retrieval:
- a. Right-click the class and click **Properties**.
  - b. Click the **Property Definitions** tab.
  - c. Click the string property you want to enable for CBR indexing and click **Edit**.
  - d. Check **CBR Enabled** and click **OK**.
  - e. Click **OK**.
10. Repeat 5 on page 99 through 9 for each additional object store to which you want to assign a CBR locale.

“Enabling additional K2 index servers and search servers”

If you add additional K2 Index Servers or Search Servers to an existing configuration, you must enable them through Enterprise Manager to utilize them.

## Enabling additional K2 index servers and search servers

If you add additional K2 Index Servers or Search Servers to an existing configuration, you must enable them through Enterprise Manager to utilize them.

1. Log on to Enterprise Manager as the GCD Administrator and expand the Enterprise Manager tree.
2. Open the Index Area folder.
3. Right-click the index area that you want to add the new services to and select *Properties*.
4. Enable the new Search Servers as follows:
  - a. Click **Edit Search Servers**.

- b. In the Search Servers Available pane, highlight any servers you want to enable for this index area and click **Add** to add the server to the Search Servers Selected list.
    - c. Click **OK** to save the settings and enable the new servers.
  5. Enable the new Index Servers as follows:
    - a. Click **Edit Index Servers**.
    - b. In the Index Servers Available pane, Highlight any servers you want to enable for this index area and click **Add** to add the server to the Index Servers Selected list.
    - c. Click **OK** to save the settings and enable the new servers.

---

## Verifying the Content Search Engine installation

To verify that the Content Search Engine installation and configuration succeeded, perform the following procedure.

To verify the Content Search Engine installation:

1. In Enterprise Manager, access the Root Folder and open a subfolder that contains a document. The document must contain text; it cannot be an image.
2. Right-click a document and select **All Tasks** → **Index for Content Search**.  
A Notice indicates that a content search index Job was created successfully.
3. Right-click the object store node for the document you set to index for content search and select **All Tasks** → **Index Jobs Management**.
4. In the Index Jobs Manager, check to see that the Job Status indicates the job has terminated normally.

Depending on the size of the indexing job, it might take a few minutes for the indexing job to complete. If the Job Status indicates that the indexing is in progress, wait a few minutes to give the job time to complete. If the Job Status does not indicate progress, check the `p8_server_error.log` file on the application server.



---

## Installing and configuring Process Engine

Installing and configuring Process Engine is a process requiring multiple steps, and the steps must be followed in sequence.

The following steps must be completed in order to install Process Engine software, configure Process Engine on the IBM FileNet P8 Platform and install the latest software updates.

1. "Installing Process Engine"  
You can install Process Engine software either interactively or silently. A number of configuration steps follow the execution of the Process Engine installation program.
2. "Installing the latest Content Engine client files on Process Engine servers" on page 116  
Installing the Content Engine Client files on all Process Engine enables communication between the Content Engine and the Process Engine. You can install these files interactively by using the installation wizard or silently by using the command line and a silent input file.
3. "Configuring Process Task Manager" on page 119  
Start the Process Task Manager and set initial configuration parameters on the Process Engine.
4. "Verifying connection to the Process Engine database" on page 121  
To verify the connection to the Process Engine database, issue the **vwcamp** command.
5. "Completing post-installation Process Engine configuration (Windows only)" on page 121  
You must enable Process Engine to use the largest available contiguous free memory area for shared memory allocations. Otherwise, at some point during normal execution, the system fails to allocate shared memory and ceases to function correctly.
6. "Installing Process Engine software updates" on page 122  
You can install software updates such as modified releases, fix packs, or interim fixes to Process Engine.

---

## Installing Process Engine

You can install Process Engine software either interactively or silently. A number of configuration steps follow the execution of the Process Engine installation program.

You will find references to logging on as the root and fnsw users within the following procedures. For all UNIX operating systems, the root user must run in the Bourne or Korn shell and the fnsw user must run in the Korn shell.

**Important:** Before starting the Process Engine installation, verify that you have completed the steps in Configuring the /etc/hosts file.

1. "Verifying the Process Engine database connection" on page 104  
Verify the ability to connect to the Process Engine database. The Process Engine installation program will connect to the database during software installation.
2. "Installing Process Engine interactively" on page 106  
Use these procedures to install Process Engine using the installation wizard screens included with the installation package.

3. "Installing Process Engine silently" on page 108  
Modify the silent installation response file according to the values in the installation worksheet before installing the software.
4. "Resetting administrative user passwords" on page 111  
Process Engine installation automatically sets the passwords for several internally required local users. For Oracle and SQL Server databases, if default users and passwords were configured, Process Engine installation also creates several database users.
5. "Verifying the connection to the Process Engine database" on page 113  
Verify the ability to connect to the Process Engine database after installing the software.
6. "Completing Oracle post-installation steps" on page 114  
Complete additional steps after installing Process Engine with an Oracle database.
7. "Completing post-installation steps on UNIX platforms" on page 114  
There are additional steps required to complete installation of Process Engine on all UNIX platforms.
8. "Completing post-installation steps on Windows platforms" on page 116  
There are additional steps required to complete installation of Process Engine on all Windows platforms.

## Verifying the Process Engine database connection

Verify the ability to connect to the Process Engine database. The Process Engine installation program will connect to the database during software installation.

"Verifying the Process Engine database connection (Oracle)"

Verify that the Oracle database instance used by Process Engine is accessible. How you log on to sqlplus will vary, depending upon how you will choose to execute the SQL scripts. Make whatever corrections are necessary before proceeding.

"Verifying the Process Engine database connection (SQL Server)" on page 105

Verify that the Microsoft SQL Server database instance used by Process Engine is accessible. You must know both the Process Engine database and filegroup names. Make whatever corrections are necessary before proceeding.

"Verifying the Process Engine database connection (DB2)" on page 106

Verify that the DB2 database used by Process Engine is accessible. You must know either the Process Engine database alias or instance name, depending on whether the database is DB2® for Linux, UNIX and Windows or DB2 for z/OS®. Make whatever corrections are necessary before proceeding.

### Verifying the Process Engine database connection (Oracle)

Verify that the Oracle database instance used by Process Engine is accessible. How you log on to sqlplus will vary, depending upon how you will choose to execute the SQL scripts. Make whatever corrections are necessary before proceeding.

This procedure will verify that you can connect to the Oracle database in the same way the Process Engine installation program will. Make whatever corrections are necessary before proceeding.

To verify the Process Engine database connection:

1. Run the following at a command prompt on the Process Engine:  
`su - oracle -c "sqlplus"`
2. Enter one of the following commands at the SQLPlus prompt, as follows:



- If the Process Engine pre-installation SQL scripts will be run from the Process Engine installation program by prompting for the sys password, type the following command:  
`sys/password as sysdba`
  - If the SQL scripts will be run from the Process Engine installation program by using operating system authentication, type the following command:  
`/ as sysdba`
3. At the prompt, enter the following SQL command:
- ```
SQL> select instance_name, host_name, version
from v$instance;
```
- The following represents an example of the information returned:
- ```
INSTANCE_NAME

HOST_NAME

VERSION

p8dbshr HQVWBUCS 10.2.0.2.0
where:
```
- *p8dbshr* is the instance ORACLE\_SID.
  - *HQVWBUCS* is the database server name.
  - *10.2.0.2.0* is the Oracle server version.

### Verifying the Process Engine database connection (SQL Server)

Verify that the Microsoft SQL Server database instance used by Process Engine is accessible. You must know both the Process Engine database and filegroup names. Make whatever corrections are necessary before proceeding.

1. Log on to the Process Engine as a member of the local Administrators group or a user with equivalent permissions. The user you log on as must also be a database administrator. If the database is remote, the SQL connection must also be a trusted connection.
2. At a command prompt, enter:  
`osql -E -D DSN`  
where *DSN* is the ODBC data source name  
This command puts Process Engine into osql interactive mode.
3. At the osql prompt, enter:  
`1> use VWdb`  
`2> go`  
where *VWdb* is the Process Engine database name  
This command verifies that the Process Engine database has been created. If you get another prompt with no error, you are attached to that database.
4. Verify that the correct Process Engine filegroup was created. At the osql prompt, enter:  
`1> select substring(groupname,1,20) from sysfilegroups where groupname='defined filegroup'`  
`2> go`  
where *defined filegroup* is the default filegroup  
A listing of the Process Engine filegroups will display, for example:  

```
vwdata_fg
```

5. Exit `osql` by typing `exit`.

## Verifying the Process Engine database connection (DB2)

Verify that the DB2 database used by Process Engine is accessible. You must know either the Process Engine database alias or instance name, depending on whether the database is DB2 for Linux, UNIX and Windows or DB2 for z/OS. Make whatever corrections are necessary before proceeding.

1. Log on to the DB2 Control Center tool on the Process Engine, as follows:

### Windows

At a command prompt, start the DB2 Command Line Processor by typing the following command:

```
db2cmd
```

and, at the subsequently displayed prompt, enter the following command:

```
db2
```

**UNIX** Log on as the client instance owner and run the following at a command prompt:

```
db2
```

2. At the DB2 prompt, enter the following command indicating either the database alias or the instance name:

```
connect to database_alias or instance_name user f_sw using
f_sw password
```

where:

*database\_alias* is the Process Engine DB2 for Linux, UNIX and Windows database alias for remote databases. For local databases, use the database name.

*instance\_name* is the Process Engine DB2 for z/OS database name

*f\_sw* is the Process Engine runtime user, either the default `f_sw` user or the assigned alias

*f\_sw password* is the runtime user's password.

DB2 will display the database connection information.

The following example shows the database connection command and the information returned:

```
db2 => connect to pedbinst user f_sw using fswpassword
```

```
Database Connection Information
```

```
Database server = DB2/AIX64 9.5.0
```

```
SQL authorization ID = F_SW
```

```
Local database alias = PEDBINST
```

In this example, the database alias is `pedbinst`, the user is `f_sw`, and the `f_sw` user password is `fswpassword`.

## Installing Process Engine interactively

Use these procedures to install Process Engine using the installation wizard screens included with the installation package.

You will find references to logging on as the `root` and `fns` users within the procedures to install Process Engine software. For all UNIX operating systems, the `root` user must run in the Bourne or Korn shell and the `fns` user must run in the Korn shell.

**Important:** Before starting the Process Engine installation, verify that you have completed the steps in the To configure your /etc/hosts file section in the *Plan and Prepare Your Environment for IBM FileNet P8*.

“Installing the Process Engine software interactively (Windows)”

You can install Process Engine by using the Process Engine installation wizard.

“Installing the Process Engine software interactively (UNIX)”

You can install Process Engine by using the Process Engine installation wizard.

## Installing the Process Engine software interactively (Windows)

You can install Process Engine by using the Process Engine installation wizard.

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 Process Engine values, filter by **PE Installer** in the **Installation or Configuration Program** column.

2. Log on to the Process Engine server as *fnsfw*, *pe\_install\_user\_domain*, or *pe\_install\_user\_local*.
3. Navigate to the Process Engine software package, and start the P8PE-4.5.1-WIN.exe installation program. To run the Process Engine installation from disk, you must copy the installation files to a disk volume where 8.3 name generation is enabled, or if 8.3 name generation is disabled, you must copy the installation to a path that uses only short (8.3) names.

When running from disk, either interactively or silently, be aware that the Process Engine installation program has a 64-character path limitation when the path is expressed in 8.3 format. This limitation applies to the IMSInst subdirectory. For example, the original path is:

```
\\server08\Software\InstallationDisks\FileNet\Release P8
4.5.1\ProcessEngine\Windows\IMSInst
```


When expressed in 8.3 format the path might be:

```
\\server08\Software\INSTAL~1\FileNet\RELEAS~1.0\PROCES~1\Windows\IMSInst
```

This compressed path is 73 characters long, exceeding the 64-character limit.

4. Check for any .log files that were generated when the installation program ran. The files could be in any of the following locations, depending on whether the installation was successful and, if not, where errors occurred. Correct any errors or failures indicated before proceeding to the next step.
  - C:\Program Files\IBM\FileNet\PE\PE451\_setup.log
  - C:\Program Files\IBM\FileNet\PE
  - C:\FNSW\tmp\_installer
  - C:\Program Files\IBM\FileNet\IS\mini\_installer.log, Windows Event logs, and log files under \FNSW\_LOC\logs
  - For 64-bit Windows, these paths will be C:\Program Files(x86)\..

### 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 Process Engine software interactively (UNIX)

You can install Process Engine by using the Process Engine installation wizard.

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 Process Engine values, filter by **PE Installer** in the **Installation or Configuration Program** column.

2. Log on to the Process Engine server as the root user. If you plan to run the SQL scripts from the Process Engine installation program, you must log on as a database administrator.
3. (AIX only) Execute the following:  
slibclean
4. Start the installation program.

Platform	Command
AIX	P8PE-4.5.1-AIX.BIN
HPUX	P8PE-4.5.1-HPUX.BIN
HPUXi	P8PE-4.5.1-HPUXI.BIN
Solaris	P8PE-4.5.1-SOL.BIN

5. Monitor `/fnsw/local/logs/wizard` to check the progress of the installation since the installation program will run for several minutes, and its progress, though displayed, might not visibly advance for an extended period of time.
6. Check for any `.log` files that were generated when the installation program ran. The files could be in any of the following locations, depending on whether the installation was successful and, if not, where errors occurred. Correct any errors or failures indicated before proceeding to the next step.
  - `/fnsw/local/logs/PE` (if the install completes successfully)
  - `/fnsw/tmp_installer/PE451_setup.log` (if the install has errors)
  - `/fnsw/local/logs/wizard/date_time.log` and other subdirectories under `/fnsw/local/logs`
7. Log off as the root user and log on as `fnsfw`.

#### 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 Process Engine silently

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

**Important:** Before starting the Process Engine installation, verify that you have completed the steps in the To configure your `/etc/hosts` file section in the *Plan and Prepare Your Environment for IBM FileNet P8*.

“Installing the Process Engine software silently (Windows)” on page 109

Complete the following procedures to silently install Process Engine.

“Installing the Process Engine software silently (UNIX)” on page 109

Complete the following procedures to silently install Process Engine.

“Encrypting passwords for Process Engine” on page 110

Several passwords are required to configure Process Engine components. To accommodate your security requirements, you can encrypt these passwords before you enter them into the configuration files.

## Installing the Process Engine software silently (Windows)


Complete the following procedures to silently install Process 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 Process Engine values, filter by **PE Installer** in the **Installation or Configuration Program** column.

2. Log on to the Process Engine server as *fnszw*, *pe\_install\_user\_domain*, or *pe\_install\_user\_local*.
3. Navigate to the Process Engine software package.
4. Edit the `PE_silent_install.txt` file to reflect the appropriate responses for your installation. All passwords in the response file must be encrypted. See “Encrypting passwords for Process Engine” on page 110 for information on use of the password encryption tool.
5. Save the edited response file to your temporary directory.
6. Navigate to the temporary directory on the local disk.
7. Open a command prompt and start the installation program:  
`P8PE-4.5.1-WIN.exe -silent -options PE_silent_install.txt`
8. Check for any `.log` files that were generated when the installation program ran. The files could be in any of the following locations, depending on whether the installation was successful and, if not, where errors occurred. Correct any errors or failures indicated before proceeding to the next step.
  - `C:\Program Files\IBM\FileNet\PE\PE451_setup.log`
  - `C:\Program Files\IBM\FileNet\PE`
  - `C:\FNSW\tmp_installer`
  - `C:\Program Files\IBM\FileNet\IS\mini_installer.log`, Windows Event logs, and log files under `\FNSW_LOC\logs`
  - For 64-bit Windows, these paths will be `C:\Program Files(x86)\..`

### 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 Process Engine software silently (UNIX)

Complete the following procedures to silently install Process 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 Process Engine values, filter by **PE Installer** in the **Installation or Configuration Program** column.


2. Log on to the Process Engine server as the root user. If you plan to run the SQL scripts from the Process Engine installation program, you must log on as a database administrator.
3. (AIX only) Execute the following:  
`slibclean`
4. Edit the `PE_silent_install.txt` file to reflect the appropriate responses for your installation. All passwords in the response file must be encrypted. See “Encrypting passwords for Process Engine” on page 110 for information on use of the password encryption tool.
5. Save the edited response file to your temporary directory.

6. Navigate to the temporary directory on the local disk.
7. From the console, launch the appropriate P8PE-4.5.1-*platform*.bin installation program.

Platform	Command
AIX	P8PE-4.5.1-AIX.BIN -silent -options PE_silent_install.txt
HPUX	P8PE-4.5.1-HPUX.BIN -silent -options PE_silent_install.txt
HPUXi	P8PE-4.5.1-HPUXI.BIN -silent -options PE_silent_install.txt
Solaris	P8PE-4.5.1-SOL.BIN -silent -options PE_silent_install.txt

8. Monitor /fnsw/local/logs/wizard to check the progress of the installation since the installation program will run for several minutes, and its progress, though displayed, might not visibly advance for an extended period of time.
9. Check for any .log files that were generated when the installation program ran. The files could be in any of the following locations, depending on whether the installation was successful and, if not, where errors occurred. Correct any errors or failures indicated before proceeding to the next step.
  - /fnsw/local/logs/PE (if the install completes successfully)
  - /fnsw/tmp\_installer/PE451\_setup.log (if the install has errors)
  - /fnsw/local/logs/wizard/date\_time.log and other subdirectories under /fnsw/local/logs
10. Log off as the root user and log on as *fnsw*.

### 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*.

## Encrypting passwords for Process Engine

Several passwords are required to configure Process Engine components. To accommodate your security requirements, you can encrypt these passwords before you enter them into the configuration files.

Ensure that Java is installed and that the location to your Java runtime environment (JRE) is in your PATH environment variable.

1. Copy the following files from the \Tools directory on the installation media for Process Engine software to a local drive:
  - fncryptutils - an executable .jar file
  - RunEncryptApp - a batch file
2. Run one of the following executable files to start the password application:

Option	Description
Windows	RunEncryptApp.bat
UNIX	RunEncryptApp.sh

3. Enter the appropriate values for the user name and password.
4. Reenter the password to confirm it.
5. Click **Generate**.

6. An encrypted password will be generated and displayed in the encrypted password field.
7. Copy and paste this password into the appropriate configuration file.

## Resetting administrative user passwords

Process Engine installation automatically sets the passwords for several internally required local users. For Oracle and SQL Server databases, if default users and passwords were configured, Process Engine installation also creates several database users.

The Process Engine installation program creates an encrypted version of the passwords for the *f\_sw* and *f\_maint* users. The encrypted version of the password must match the database or operating system passwords for these users. If the passwords do not match, Process Engine will fail to connect to the database. If these users are created with default passwords, it is a best practice to reset the passwords for these users.

For the *fns* operating system user, on a Windows server, the password entered during Process Engine installation must match the operating system password. If these passwords do not match, Process Engine services on the Windows server will not start.

The following table lists the users, the level of system access each user has, and the tool used to change the password.

User Name	User Type	Description	How to modify
<i>f_sw</i>	<ul style="list-style-type: none"> <li>• Database (Oracle, SQL)</li> <li>• OS user for DB2</li> </ul>	Has privileges only for database objects created by Process Engine. Used as the Process Engine runtime user.	Execute <code>xdbcconnect</code> .
<i>f_maint</i>	<ul style="list-style-type: none"> <li>• Database (Oracle, SQL)</li> <li>• OS user for DB2</li> </ul>	Has DBA privileges. Used for RDBMS maintenance.	Execute <code>xdbcconnect</code> .



User Name	User Type	Description	How to modify
<i>fnsfw</i>	Operating System	Primary Process Engine user. Used to execute Process Engine software and services.	<p>The <i>fnsfw</i> user is configured by the installation program to start the following Windows services:</p> <ul style="list-style-type: none"> <li>• IMS™ ControlService</li> <li>• Process Engine Services Manager</li> </ul> <p>If you change the password for the <i>fnsfw</i> user, you must also use the Windows Services tool to update the password on the Log On tab for these services.</p> <p>Process Engine activity will cease if the <i>fnsfw</i> user's password expires.</p>

**“Setting the *f\_maint* and *f\_sw* passwords (Oracle and Microsoft SQL Server)”**

For added security, Process Engine stores an encrypted version of the passwords for the *f\_sw* and *f\_maint* users, or their aliases, in a file called *rdbup.bin*. This is in addition to passwords for these users in the Oracle or Microsoft SQL Server database. The encrypted password and the database user's passwords must match.

**“Setting the *f\_maint* and *f\_sw* passwords (DB2)” on page 113**

For added security, Process Engine stores an encrypted version of the passwords for the *f\_sw* and *f\_maint* users, or their aliases, in a file called *rdbup.bin*.

**Setting the *f\_maint* and *f\_sw* passwords (Oracle and Microsoft SQL Server)**

For added security, Process Engine stores an encrypted version of the passwords for the *f\_sw* and *f\_maint* users, or their aliases, in a file called *rdbup.bin*. This is in addition to passwords for these users in the Oracle or Microsoft SQL Server database. The encrypted password and the database user's passwords must match.

To verify that the passwords match between the encrypted file and the Oracle or SQL Server database, use the following procedure to start the Xdbconnect utility. Xdbconnect works only if the passwords in the encrypted file and the database match.

You must change the passwords for the *f\_maint* and *f\_sw* users. For Oracle and Microsoft SQL Server databases, both the encrypted file and the database passwords are updated.

On UNIX, several Process Engine utilities are configured with *setuid fnsfw*. (or its alias), and will therefore run with that user's X Window settings, regardless of which user is currently logged on.

1. Log on as the *fnsfw* user.

2. Start the Database Server Connect application by running the following command: `Xdbconnect -r`
3. Change the primary password for the users `f_sw` and `f_maint` to match the database password.
4. Exit the application.

### Setting the `f_maint` and `f_sw` passwords (DB2)

For added security, Process Engine stores an encrypted version of the passwords for the `f_sw` and `f_maint` users, or their aliases, in a file called `rdbup.bin`.

To verify that the passwords match between the encrypted file and the operating system, you can use the `Xdbconnect` utility. `Xdbconnect` works only if the passwords in the encrypted file and the database match.

You must change the passwords for the `f_maint` and `f_sw` users. For DB2, the encrypted file will be updated.

On UNIX, several Process Engine utilities are `setuid fnsw` (or its alias), and will therefore run with that user's X Window settings regardless of which user is currently logged on.

1. Log on as the `fnsw` user.
2. Start the Database Server Connect application by executing the following:  
`Xdbconnect -r`
3. Change the primary password for the users `f_sw` and `f_maint` to match the operating system user password.
4. Exit the application.

## Verifying the connection to the Process Engine database

Verify the ability to connect to the Process Engine database after installing the software.

Restart the software and initiate a connection to the Process Engine database. This connection will use the database runtime user name and password as defined when Process Engine was installed and configured. This will verify the ability to use that name and password to connect to the database.

1. Open a command window and restart the Process Engine software by executing the following commands at a command prompt:

```
initfnsw -y stop
killfnsw -DAyS
initfnsw -y start
```

**Note:** If Process Engine is on an AIX server, delete the following files after the `killfnsw` command and before `initfnsw -y start`:

- `/fnsw/local/sd/1/NUM_SEG`
- `/fnsw/local/sd/1/SHM_MB`

2. Initiate the connection to the database. At a command prompt, execute:  
`wcemp -l`

where `-l` lists the current configuration information for the Content Engine connection

If the connection is successful, you will see a message indicating that the Content Engine has not been configured yet. Because there are no security settings

configured, the above command should return a message similar to The Process Engine's connection to the Content Engine has not been configured....

Unsuccessful connection to the database will return an exception.

If the connection is not successful, there could be a mismatch between the password entered for the `f_sw` user during Process Engine installation and the password created by execution of the SQL scripts (Oracle) or for the operating system runtime user (DB2).

To determine if a failure to connect to the database is due to a password mismatch, use the steps in:

- “Setting the `f_maint` and `f_sw` passwords (Oracle and Microsoft SQL Server)” on page 112
- “Setting the `f_maint` and `f_sw` passwords (DB2)” on page 113

## Completing Oracle post-installation steps

Complete additional steps after installing Process Engine with an Oracle database.

“Re-enabling Oracle password complexity verification”

If, as directed earlier, you disabled the Oracle Password Complexity Verification feature prior to installing Process Engine, you can now re-enable it.

### Re-enabling Oracle password complexity verification

If, as directed earlier, you disabled the Oracle Password Complexity Verification feature prior to installing Process Engine, you can now re-enable it.

## Completing post-installation steps on UNIX platforms

There are additional steps required to complete installation of Process Engine on all UNIX platforms.

“Restoring any custom modifications for root and `fns` users (UNIX)”

Process Engine installation creates new versions of a number of files, and if the previous versions of these files contained any custom settings, they must be restored.

“Cleaning up before starting Process Engine (UNIX)” on page 115

You must run the `killfns` command before starting Process Engine.

“Editing the `/etc/inittab` file (UNIX)” on page 115

By default, the Process Engine software starts automatically when you restart the server and needs its database started beforehand.

“Modifying the network configuration (UNIX)” on page 116

Create a touch file to force Image Services to use the IPv4 protocol.

### Restoring any custom modifications for root and `fns` users (UNIX)

Process Engine installation creates new versions of a number of files, and if the previous versions of these files contained any custom settings, they must be restored.

Edit the new files for the `fns` and root users accordingly. Saved files are in `.filename.old.nn`, where `nn` is a sequential number. The latest saved version will be in the highest numbered file. The following files are modified by the Process Engine installation program:

`.xdefaults`

```
.Xresources
.dbxinit
.dtpofile
.env
.login
.mwmrc
.xinitrc
.profile
.cshrc
```

## Cleaning up before starting Process Engine (UNIX)

You must run the `killfnsw` command before starting Process Engine.

1. Log on as `fnsw`.
2. Execute:  
`killfnsw -DAyS`
3. Execute:  
`ipcs -a`
4. Verify there is no entry with `0x464` pattern. If there are any entries with this pattern, use `ipcrm` to remove them.

## Editing the `/etc/inittab` file (UNIX)

By default, the Process Engine software starts automatically when you restart the server and needs its database started beforehand.

If the database is not automatically started on server restart, edit the `/etc/inittab` file on the Process Engine machine to comment out the autostart of Process Engine. The following are examples of changes to make.

### AIX Change:

```
rcfnsw:2:once:/etc/rc.initfnsw 2>&1 | alog
-tboot > /dev/console 2>&1
```

to read:

```
:rcfnsw:2:once:/etc/rc.initfnsw 2>&1 | alog
-tboot > /dev/console 2>&1
```

### HP-UX

Change:

```
rcfn:2:once:/etc/rc.initfnsw 2>&1 | alog
-tboot > /dev/console 2>&1
```

to read:

```
#rcfn:2:once:/etc/rc.initfnsw 2>&1 | alog -tboot > /dev/console 2>&1
```

### Solaris

Change:

```
fn:3:wait:/bin/sh /etc/rc.initfnsw
</dev/console >/dev/console 2>&1
```

to read:

```
#fn:3:wait:/bin/sh /etc/rc.initfnsw
</dev/console >/dev/console 2>&1
```

## Modifying the network configuration (UNIX)

Create a touch file to force Image Services to use the IPv4 protocol.

If the Process Engine is configured to support both IPv6 and IPv4 protocol, you can force Process Engine to use IPv4. To use the IPv4 protocol, create an empty file in the `/fnsw/local/sd` directory. If the file is present, the Process Engine software will override the default and use the IPv4 protocol.

1. Navigate to the `/fnsw/local/sd` directory.
2. Create an empty file and save it as a file named `ipv4`. Verify that there is no file extension on the file.

## Completing post-installation steps on Windows platforms

There are additional steps required to complete installation of Process Engine on all Windows platforms.

“Modifying the network configuration (Windows 2008)”

Create a touch file to force Image Services to use the IPv4 protocol.

“Modifying the integrity level for executables (Windows 2008)”

Modify the mandatory integrity level of the Image Services executables to **High**.

### Modifying the network configuration (Windows 2008)

Create a touch file to force Image Services to use the IPv4 protocol.

Windows 2008 supports both IPv6 and IPv4 protocols. By default, the preferred protocol is IPv6. To use the IPv4 protocol, create an empty file in the `\fnsw_loc\sd` directory. If the file is present, the Process Engine software will override the Windows default and use the IPv4 protocol.

1. Navigate to the `C:\FNSW_LOC\sd` directory.
2. Using an editor such as Notepad, create an empty file and save it as a file named `ipv4`. Verify that there is no file extension on the file.

### Modifying the integrity level for executables (Windows 2008)

Modify the mandatory integrity level of the Image Services executables to **High**.

Complete the following procedure:

1. Open a command prompt with Administrative privileges.
2. Change the current directory to `installLocation\fnsw\bin`.
3. Execute the following command:

```
icacls *.exe /setintegritylevel H
```

---

## Installing the latest Content Engine client files on Process Engine servers

Installing the Content Engine Client files on all Process Engine enables communication between the Content Engine and the Process Engine. You can install these files interactively by using the installation wizard or silently by using the command line and a silent input file.

“Installing the latest Content Engine client files on Process Engine servers interactively” on page 117

The installation wizard provides an interactive way to install the Content 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 Engine client files on Process Engine servers silently” on page 118

The command line method provides a way to silently install the Content 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 Content Engine parameter values, see *Plan and Prepare Your Environment for IBM FileNet P8*.

## Installing the latest Content Engine client files on Process Engine servers interactively

The installation wizard provides an interactive way to install the Content Engine Client files. You can use the values from your worksheet to fill in the required value for each field on the wizard screens.

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

To install the Content Engine Client 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 Content Engine values, filter by **CE Client Installer** in the **Installation or Configuration Program** column.

2. To download the latest software updates, and to determine which of these updates might be required for use with other components and expansion products, contact your service representative.
3. On the machine where Process Engine is installed, log on as `fns`, with these permissions:
  - Read and write permission to a temporary directory, such as `temp` (Windows) or `tmp` (UNIX), on the machine where Process Engine is installed
  - Execute permission on the Content Engine Client install software

The default password for `fns` was `BPMtemp1pzd`.

4. Verify that there is a current backup of Process Engine.
5. Copy the Content Engine Client installation software from the Content Engine installation software to the temporary directory. The version of the client installation software must match the version of Content Engine.
6. Expand the compressed Content Engine Client installation software file in the temporary directory.
7. Access the IBM FileNet Content Engine Client update software in the temporary directory.
8. Run the following command:


Operating System	Install Program
AIX	P8CE-CLIENT-4.5.1-AIX.BIN
HPUX	P8CE-CLIENT-4.5.1-HPUX.BIN
HPUXi	P8CE-CLIENT-4.5.1-HPUXI.BIN
Linux	P8CE-CLIENT-4.5.1-LINUX.BIN
Solaris	P8CE-CLIENT-4.5.1-SOL.BIN

Operating System	Install Program
Windows	P8CE-CLIENT-4.5.1-WIN.EXE
Linux on System z	P8CE-CLIENT-4.5.1-ZLINUX.BIN

- Complete the installation program wizard by using the values from your worksheet.
- When the installation completes, check the Content 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 Engine Client files:

Operating System	Path to Log File
UNIX	/opt/IBM/FileNet/CEClient/ ceclient_install_log_4_5_1.txt
Windows	C:\Program Files\IBM\FileNet\CEClient\ ceclient_install_log_4_5_1.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 Engine client files on Process Engine servers silently

The command line method provides a way to silently install the Content 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.

To install the Content Engine Client files:

- 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 **CE Client Installer** in the **Installation or Configuration Program** column.

- To download the latest software updates, and to determine which of these updates might be required for use with other components and expansion products, contact your service representative.
- On the machine where Process Engine is installed, log on as fnsw, with these permissions:
  - Read and write permission to a temporary directory, such as *temp* (Windows) or *tmp* (UNIX), on the machine where Process Engine is installed
  - Execute permission on the Content Engine Client install software

The default password for fnsw was BPMtemp1pzwd.
- Verify that there is a current backup of Process Engine.
- Copy the Content Engine Client installation software from the Content Engine installation software to the temporary directory. The version of the client installation software must match the version of Content Engine.
- Expand the compressed Content Engine Client installation software file in the temporary directory.



7. Make a backup copy of the CEClient\_silent\_install.txt input file in the temporary directory.
8. 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.
9. Navigate to the temporary directory path containing the Content Engine Client installation program, and run the following command, where:
 


*path* is the path that contains the installation program.

Operating System	Install Program
AIX	P8CE-CLIENT-4.5.1-AIX.BIN -f <i>path</i> /CECLIENT.AIX/ CEClient_silent_install.txt -i silent
HPUX	P8CE-CLIENT-4.5.1-HPUX.BIN -f <i>path</i> /CEClient.HPUX/ CEClient_silent_install.txt -i silent
HPUXi	P8CE-CLIENT-4.5.1-HPUXI.BIN -f <i>path</i> /CEClient.HPUXI/ CEClient_silent_install.txt -i silent
Linux	P8CE-CLIENT-4.5.1-LINUX.BIN -f <i>path</i> /CEClient.Linux/ CEClient_silent_install.txt -i silent
Solaris	P8CE-CLIENT-4.5.1-SOL.BIN -f <i>path</i> /CEClient.Solaris/ CEClient_silent_install.txt -i silent
Windows	P8CE-CLIENT-4.5.1-WIN.EXE -f <i>path</i> \CEClient.Windows\ CEClient_silent_install.txt -i silent
Linux on System z	P8CE-CLIENT-4.5.1-ZLINUX.BIN -f <i>path</i> /CEClient.zLinux/ CEClient_silent_install.txt -i silent

10. When the installation completes, check the Content 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 Engine Client files:

Operating System	Path to Log File
UNIX	/opt/IBM/FileNet/CEClient/ ceclient_install_log_4_5_1.txt
Windows	C:\Program Files\IBM\FileNet\CEClient\ ceclient_install_log_4_5_1.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 Process Task Manager

Start the Process Task Manager and set initial configuration parameters on the Process 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 Process Engine values, filter by **Process Task Manager** in the **Installation or Configuration Program** column.

2. Log on to the Process Engine server as *fnsfw*.
3. Start the Process Task Manager, as follows:

Option	Description
Windows	Select <b>Start</b> → <b>Programs</b> → <b>IBM FileNet P8 Platform</b> → <b>Process Engine</b> → <b>Process Task Manager</b> .
UNIX	Enter <code>vwtaskman</code> at the command prompt. The terminal should support X Windows and the <code>DISPLAY</code> environment variable should be set.

4. Right-click your Process Engine server in the left-hand pane and start the software if it is not already running.
5. Select the Process Engine in the feature pane and click the **Security** tab to configure the Security settings.  
Provide the service username, entered as a short name, the Content Engine URI, Administrator Group, and Configuration Group identified on your installation worksheet. See the IBM FileNet P8 help topic *System Administration > Enterprise-wide Administration > Process Task Manager > Process Engine > Configure Process Engine > Security* for details on the user and groups.
6. Click the **General** tab and make sure all settings are correct. Click **Apply** if any changes had been made.  
After all parameters have been entered, click **Apply** and restart the Process Service when prompted. If errors are returned, additional information is available in the following file. If no errors are returned, the file will not exist.

Option	Description
Windows	<code>\fnsw_loc\logs\TM_daemon\PEDirectoryServerConnectionDebug.txt</code>
UNIX	<code>/fnsw/local/logs/TM_daemon/PEDirectoryServerConnectionDebug.txt</code>

7. Right-click on the **Regions** folder, in the left-hand pane and select **New** to create a new region. See the IBM FileNet P8 help topic *System Administration > Isolated Regions > Concepts* for information on isolated regions.
8. Select the **General** subtab and fill in a region number. Use any number between 1 and 999 that has not already been used.
9. Indicate whether region recovery will be enabled for this region. If you will be using region recovery, identify the tablespaces or filegroups to be used by the region.
10. Click the **Security** subtab to set a region password.  
**Important:** You will use this password later when you create a Process Engine Region in “Creating a Process Engine isolated region” on page 165.
11. After all parameters have been entered, click **OK**.
12. When prompted by Process Task Manager to start the software, click **OK**. Process Task Manager will start the software automatically by executing:  
`initfnsw -y restart`

13. If the Process Engine server will be configured to run both IPv4 and IPv6 protocols, restart the Process Task Manager and complete the following sub-steps.

a. Select the Process Engine node.

a. On the Advanced page, add the `vworbbroker.endPoint` property:

```
vworbbroker.endPoint = iiop://1.2@pe_server_ipv6_address
:port#,pe_server_ipv4_address:port#
/hostname_in_ior=loadbalancer_virtual_name
```

Where:

- `pe_server_ipv6_address` is the IPv6 address of the Process Engine Server. The format entered in the string for an IPv6 address must have the IPv6 address enclosed in square brackets '[' ']' For example: `[2007::9:181:124:200]`
- `pe_server_ipv4_address` is the address of the Process Engine server in IPv4 format.
- `loadbalancer_virtual_name` is the name of the load balancer, used by the clients with the Process Engine server.
- The address and port pairs are separated by a comma.

---

## Verifying connection to the Process Engine database

To verify the connection to the Process Engine database, issue the `vwccmp` command.

Check the database connection from Process Engine by executing the following from a command prompt. This will also verify that security settings were saved to the database.

```
vwccmp -l
```

If the security settings were saved, the above command will return the information you entered in the Process Task Manager.

If there are no security settings configured, the above command should return a message similar to "...no object service is configured...."

---

## Completing post-installation Process Engine configuration (Windows only)

You must enable Process Engine to use the largest available contiguous free memory area for shared memory allocations. Otherwise, at some point during normal execution, the system fails to allocate shared memory and ceases to function correctly.

To configure contiguous free memory for Process Engine:

1. Log on as the `fns` (or alias) user.
2. Restart the Process Engine software. At a Windows command prompt, enter:  
`initfns -y restart`
3. Find the largest available shared memory block and create an executable file with a `.reg` file extension. That file will be run to update the registry to create a new `DWORD` value.
  - a. Create the file by entering the following at a Windows command prompt:  
`set_shm_address -r shmaddress.reg` where:

- -r indicates an input file
  - *shmaddress.reg* is the name of the file that contains registry information. This file must have the .reg file extension.
- b. Verify the contents of the output file. The following are examples of the file content.

**32-bit Windows**

```
[HKEY_LOCAL_MACHINE\SOFTWARE\FileNET\IMS\CurrentVersion]
"StartShmAddress"=dword:12230000
```

**64-bit Windows**

```
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\FileNET\IMS\CurrentVersion]
"StartShmAddress"=dword:12230000
```

4. Run the executable file to update the registry by typing the following at a Windows command: *shmaddress.reg shmaddress.reg* is the file you just created.
5. Restart the Process Engine software. At a Windows command prompt, enter:  
initfnsw -y restart
6. Verify the setting that you just applied for the shared memory address by entering the following command at a command prompt: *set\_shm\_address -v*

## Installing Process Engine software updates

You can install software updates such as modified releases, fix packs, or interim fixes to Process Engine.

To install the Process Engine software updates:

1. Contact your service representative to obtain the latest Process Engine software updates, and to determine whether additional interim fixes are needed.
2. Open the readmes for the Process Engine software updates and perform the installation procedures in the readmes on the Process Engine.

---

## Installing and configuring Application Engine

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

1. "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 Engine.
2. "Installing Application Engine software updates" on page 126  
If any required fix packs and interim fixes exist for Application Engine, you must install these software updates.
3. "Installing the latest Content Engine Client files on Application Engine servers" on page 126  
The Content Engine Client software enables communication between the Application Engine and the Content Engine. Install the latest release or fix pack version of the Content Engine Client files on all Application Engine servers.
4. "Installing the latest Process Engine Client files on Application Engine servers" on page 129  
The Process Engine Client software enables communication between the Application Engine and the Process Engine. Install the Process Engine Client files on all Application Engine servers.
5. "Configuring Application Engine on the application server" on page 131  
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 Engine. You can choose the appropriate configuration tasks for your application server type and environment.
6. "Deploying Application Engine on the application server" on page 152  
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.
7. "Setting Application Engine bootstrap preferences" on page 159  
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

---

### 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 Engine.

- 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 Engine to hold the site preferences. See “Creating the initial object store” on page 76 for more information.
- You can install a new Application Engine 4.0.2 server within an existing 4.0 IBM FileNet P8 environment if your Content Engine is at version 401.006 or later and your Process Engine is at 403-000.001 or later. The Content Engine and Process Engine client files you install on the Application Engine must match the version of your Content Engine and Process Engine.

“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.

“Installing Application Engine silently” on page 125

You can include the parameters for your Application Engine installation in a silent input file, and then run the installation from a command line.

## 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.

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. Log on to the application server, as appropriate for your operating system:

Option	Description
UNIX	Log on as a user with read, write, and execute access to the directory where you plan to install Application Engine.
Windows	Log on as a member of the local Administrators group or a user with equivalent permissions.


3. Access the IBM FileNet P8 Application Engine 4.0.2.0 installation software.
4. Start the installation program.

Platform	Command
AIX	P8AE-4.0.2.0-AIX.bin
HPUX	P8AE-4.0.2.0-HPUX.bin
HPUXi	P8AE-4.0.2.0-HPUX64.bin
Linux	P8AE-4.0.2.0-LINUX.bin

Platform	Command
Solaris	P8AE-4.0.2.0-SOL.bin
Windows	P8AE-4.0.2.0-WIN.exe
Linux on System z	P8AE-4.0.2.0-ZLINUX.bin

- Complete the Application Engine installer screens by using the values from your worksheet.
- 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.

### 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 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.

To install the Application Engine software silently:

- 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.

- Log on to the application server, as appropriate for your operating system:

Option	Description
UNIX	Log on as a user with read, write, and execute access to the directory where you plan to install Application Engine.
Windows	Log on as a member of the local Administrators group or a user with equivalent permissions.

- 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.
- 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:

#### UNIX

Change `../FileNet/AE` to `../FileNet`

#### Windows



Change ..\FileNet\AE to ..\FileNet

Change ..\FileNet\AE to ..\FileNet

5. From a command prompt, navigate to and run the installer.

#### UNIX

```
./P8AE-4.0.2.0-operating system.bin -options
path_to_edited_input_file/AE_silent_input.txt -silent
```


#### Windows

```
P8AE-4.0.2.0-Win.exe -options
path_to_edited_input_file\AE_silent_input.txt -silent
```

6. 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.

#### 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 Application Engine software updates

If any required fix packs and interim fixes exist for Application Engine, you must install these software updates.

To install the Application Engine software updates:

1. To download the latest software updates, and to determine which of these updates might be required for use with other components and expansion products, contact your support representative.
2. Open the readmes for any subsequent fix packs or interim fixes (typically optional) and perform the installation procedures provided.

---

## Installing the latest Content Engine Client files on Application Engine servers

The Content Engine Client software enables communication between the Application Engine and the Content Engine. Install the latest release or fix pack version of the Content 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 Engine Client files on Application Engine servers interactively” on page 127

The installation wizard provides an interactive way to install the Content 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 Engine Client files on Application Engine servers silently” on page 128

The command-line method provides a way to silently install the Content 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 Engine Client files on Application Engine servers interactively

The installation wizard provides an interactive way to install the Content Engine Client files. You can use the values from your worksheet to fill in the required value for each field on the wizard screens.

To install the Content 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 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 (UNIX), on the machine where Application Engine is installed
  - Execute permission on the Content Engine Client install software
3. Copy the Content Engine Client installation software from the Content Engine installation software to the temporary directory. The version of the client installation software must match the version of Content Engine.
4. Expand the compressed Content Engine Client installation software file in the temporary directory.
5. Access the IBM FileNet Content Engine Client update software in the temporary directory.
6. Run the following command:

Operating System	Install Program
AIX	P8CE-CLIENT-4.5.1-AIX.BIN
HPUX	P8CE-CLIENT-4.5.1-HPUX.BIN
HPUXi	P8CE-CLIENT-4.5.1-HPUXI.BIN
Linux	P8CE-CLIENT-4.5.1-LINUX.BIN
Solaris	P8CE-CLIENT-4.5.1-SOL.BIN
Windows	P8CE-CLIENT-4.5.1-WIN.EXE
Linux on System z	P8CE-CLIENT-4.5.1-ZLINUX.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 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 Engine Client files:

Operating System	Path to Log File
UNIX	/opt/IBM/FileNet/CEClient/ ceclient_install_log_4_5_1.txt
Windows	C:\Program Files\IBM\FileNet\CEClient\ ceclient_install_log_4_5_1.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 Engine Client files on Application Engine servers silently

The command-line method provides a way to silently install the Content Engine Client files. You can use the values in your installation worksheet to edit the silent input text file before you run the installation.

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 **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 (UNIX), on the machine where Application Engine is installed
  - Execute permission on the Content Engine Client install software
3. Copy the Content Engine Client installation software from the Content Engine installation software to the temporary directory. The version of the client installation software must match the version of Content Engine.
4. Expand the compressed Content 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 Engine Client installation program, and run the following command, where:

*path* is the path that contains the installation program.


Operating System	Install Program
AIX	P8CE-CLIENT-4.5.1-AIX.BIN -f <i>path</i> /CECLIENT.AIX/ CEClient_silent_install.txt -i silent
HPUX	P8CE-CLIENT-4.5.1-HPUX.BIN -f <i>path</i> /CEClient.HPUX/ CEClient_silent_install.txt -i silent
HPUXi	P8CE-CLIENT-4.5.1-HPUXI.BIN -f <i>path</i> /CEClient.HPUXI/ CEClient_silent_install.txt -i silent

Operating System	Install Program
Linux	P8CE-CLIENT-4.5.1-LINUX.BIN -f <i>path</i> /CEClient.Linux/ CEClient_silent_install.txt -i silent
Solaris	P8CE-CLIENT-4.5.1-SOL.BIN -f <i>path</i> /CEClient.Solaris/ CEClient_silent_install.txt -i silent
Windows	P8CE-CLIENT-4.5.1-WIN.EXE -f <i>path</i> \CEClient.Windows\ CEClient_silent_install.txt -i silent
Linux on System z	P8CE-CLIENT-4.5.1-ZLINUX.BIN -f <i>path</i> /CEClient.zLinux/ CEClient_silent_install.txt -i silent

8. When the installation completes, check the Content 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 Engine Client files:

Operating System	Path to Log File
UNIX	/opt/IBM/FileNet/CEClient/ ceclient_install_log_4_5_1.txt
Windows	C:\Program Files\IBM\FileNet\CEClient\ ceclient_install_log_4_5_1.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 Process Engine Client files on Application Engine servers

The Process Engine Client software enables communication between the Application Engine and the Process Engine. Install the Process Engine Client files on all Application Engine servers.

“Installing the latest Process Engine Client files interactively”

The installation wizard provides an interactive way to install the Process Engine Client files. You can use the values you collected on your worksheet to fill in the required value for each field on the wizard screens.

“Installing the latest Process Engine Client files silently” on page 130

You can install the Process Engine Client software on the Application Engine by using a silent input text file and running the installation program from the command line. Use the values in your installation worksheet to edit the silent input text file before you run the installation.

### Installing the latest Process Engine Client files interactively

The installation wizard provides an interactive way to install the Process Engine Client files. You can use the values you collected on your worksheet to fill in the required value for each field on the wizard screens.

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


To install the Process Engine Client files:

1. On the machine where Application Engine is to be deployed, log on as any user who has the following permissions:
  - Read and write permission to a temporary directory, such as temp (Windows) or tmp (UNIX), on the machine where Application Engine is installed.
  - Execute permission on the Process Engine Client install software.
2. Copy the Process Engine Client install software from the Process Engine installation software to the temporary directory. The version of the install software must match the version of Process Engine.
3. Expand the compressed Process Engine Client install software file within the temporary directory. The `jre.tar` file that is packaged with the Process Engine Client installer must be in the same directory as the Process Engine Client installer when the installer is run. The expanded install software contains the Process Engine Client install program specific to the operating system on the machine where Application Engine is deployed.
4. Start the installation program by running the following command:

Operating System	Install Program
AIX	P8PE-CLIENT- <i>PE_version</i> -AIX.BIN
HPUX	P8PE-CLIENT- <i>PE_version</i> -HPUX.BIN
HPUXi	P8PE-CLIENT- <i>PE_version</i> -HPUXI.BIN
Linux	P8PE-CLIENT- <i>PE_version</i> -LINUX.BIN
Solaris	P8PE-CLIENT- <i>PE_version</i> -SOL.BIN
Windows	P8PE-CLIENT- <i>PE_version</i> -WIN.EXE
Linux on System z	P8PE-CLIENT- <i>PE_version</i> -ZLINUX.BIN

5. Complete the installation screens by using the values from your worksheet.
6. If the Process Engine is configured to use the IPv6 network protocol, locate and edit the `taskman.properties` file and add the following lines to that file:
  - Djava.net.preferIPv6Addresses=true
  - Djava.net.preferIPv4Stack=false

#### 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 Process Engine Client files silently

You can install the Process Engine Client software on the Application Engine by using a silent input text file and running the installation program from the command line. 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.

To install the Process Engine Client files:


1. On the machine where Application Engine is to be deployed, log on as any user who has the following permissions:

- Read and write permission to a temporary directory, such as temp (Windows) or tmp (UNIX), on the machine where Application Engine is installed.
  - Execute permission on the Process Engine Client install software.
2. Copy the Process Engine Client install software from the Process Engine installation software to the temporary directory. The version of the install software must match the version of Process Engine.
  3. Expand the compressed Process Engine Client install software file within the temporary directory. The jre.tar file that is packaged with the Process Engine Client installer must be in the same directory as the Process Engine Client installer when the installer is run. The expanded install software contains the Process Engine Client install program specific to the operating system on the machine where Application Engine is deployed.
  4. In the expanded installation software, open the file PEClient\_silent\_install.txt and change the Variable\_CheckboxAE line to:  
-V Variable\_CheckboxAE="true"
  5. Start the installation program by running the following command:

Operating System	Install Program
AIX	P8PE-CLIENT- <i>PE_version</i> -AIX.BIN -silent -options "PEClient_silent_install.txt"
HPUX	P8PE-CLIENT- <i>PE_version</i> -HPUX.BIN -silent -options "PEClient_silent_install.txt"
HPUXi	P8PE-CLIENT- <i>PE_version</i> -HPUXI.BIN -silent -options "PEClient_silent_install.txt"
Linux	P8PE-CLIENT- <i>PE_version</i> -LINUX.BIN -silent -options "PEClient_silent_install.txt"
Solaris	P8PE-CLIENT- <i>PE_version</i> -SOL.BIN -silent -options "PEClient_silent_install.txt"
Windows	P8PE-CLIENT- <i>PE_version</i> -WIN.EXE -silent -options "PEClient_silent_install.txt"
zLinux	P8PE-CLIENT- <i>PE_version</i> -ZLINUX.BIN -silent -options "PEClient_silent_install.txt"

6. If the Process Engine is configured to use the IPv6 network protocol, locate and edit the taskman.properties file and add the following lines to that file:  
-Djava.net.preferIPv6Addresses=true  
-Djava.net.preferIPv4Stack=false

#### 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 Engine. You can choose the appropriate configuration tasks for your application server type and environment.

“Configuring Application Engine on WebSphere Application Server” on page 132

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 WebLogic Server” on page 144

After you install the Application Engine server, you must configure WebLogic Server to work with Application Engine. You can also configure changes for optional modes like SSO.

“Configuring Application Engine on JBoss Application Server” on page 150

After you install the Application Engine server, you must configure JBoss 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.

“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.

“Editing web.xml for SSO” on page 135

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 139

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 140

To set up LTPA security, configure settings to match on both the Content Engine application server and the Application Engine application server. If your Application Engine and Content 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 142

To enable LDAP communication between Application Engine and Content Engine, you must configure settings on the WebSphere Application Server.

“Configuring Lightweight Directory Access Protocol (LDAP) for federated repositories” on page 143

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.

### 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`



- 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>
```

- 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 thecontainer 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>/portlets/Author/edit.jsp</url-pattern>
<url-pattern>/portlets/Author/portlet.jsp</url-pattern>
<url-pattern>/portlets/Browse/edit.jsp</url-pattern>
<url-pattern>/portlets/Browse/portlet.jsp</url-pattern>
<url-pattern>/portlets/ExternalUrl/edit.jsp</url-pattern>
<url-pattern>/portlets/ExternalUrl/portlet.jsp</url-pattern>
<url-pattern>/portlets/GroupPageDesign.jsp</url-pattern>
<url-pattern>/portlets/GroupPageSettings.jsp</url-pattern>
<url-pattern>/portlets/Inbox/edit.jsp</url-pattern>
<url-pattern>/portlets/Inbox/portlet.jsp</url-pattern>
<url-pattern>/portlets/MultiPagesDesign.jsp</url-pattern>
<url-pattern>/portlets/OrganizePages.jsp</url-pattern>
<url-pattern>/portlets/PortalPageDesign.jsp</url-pattern>
<url-pattern>/portlets/PortalPageInfo.jsp</url-pattern>
<url-pattern>/portlets/PortletAlias.jsp</url-pattern>
<url-pattern>/portlets/PortletSettings.jsp</url-pattern>
<url-pattern>/portlets/PreviewAndSetup.jsp</url-pattern>
<url-pattern>/portlets/PublicQueue/edit.jsp</url-pattern>
<url-pattern>/portlets/PublicQueue/portlet.jsp</url-pattern>
<url-pattern>/portlets/QuickSearch/edit.jsp</url-pattern>
<url-pattern>/portlets/QuickSearch/portlet.jsp</url-pattern>
<url-pattern>/portlets/Workflows/edit.jsp</url-pattern>
<url-pattern>/portlets/Workflows/portlet.jsp</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>/WcmPortletHelp.jsp</url-pattern>
<url-pattern>/WcmPortletSearch.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>/vwsimsoapservlet</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 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>

```

6. 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>

```

7. 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>

```

8. 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 thecontainer 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>/portlets/Author/edit.jsp</url-pattern>
<url-pattern>/portlets/Author/portlet.jsp</url-pattern>
<url-pattern>/portlets/Browse/edit.jsp</url-pattern>
<url-pattern>/portlets/Browse/portlet.jsp</url-pattern>
<url-pattern>/portlets/ExternalUrl/edit.jsp</url-pattern>
<url-pattern>/portlets/ExternalUrl/portlet.jsp</url-pattern>
<url-pattern>/portlets/GroupPageDesign.jsp</url-pattern>
<url-pattern>/portlets/GroupPageSettings.jsp</url-pattern>
<url-pattern>/portlets/Inbox/edit.jsp</url-pattern>
<url-pattern>/portlets/Inbox/portlet.jsp</url-pattern>
<url-pattern>/portlets/MultiPagesDesign.jsp</url-pattern>
<url-pattern>/portlets/OrganizePages.jsp</url-pattern>
<url-pattern>/portlets/PortalPageDesign.jsp</url-pattern>
<url-pattern>/portlets/PortalPageInfo.jsp</url-pattern>
<url-pattern>/portlets/PortletAlias.jsp</url-pattern>
<url-pattern>/portlets/PortletSettings.jsp</url-pattern>
<url-pattern>/portlets/PreviewAndSetup.jsp</url-pattern>
<url-pattern>/portlets/PublicQueue/edit.jsp</url-pattern>
<url-pattern>/portlets/PublicQueue/portlet.jsp</url-pattern>
<url-pattern>/portlets/QuickSearch/edit.jsp</url-pattern>
<url-pattern>/portlets/QuickSearch/portlet.jsp</url-pattern>
<url-pattern>/portlets/Workflows/edit.jsp</url-pattern>
<url-pattern>/portlets/Workflows/portlet.jsp</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>/WcmPortletHelp.jsp</url-pattern>
<url-pattern>/WcmPortletSearch.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>/vwsimsoapservlet</url-pattern>
<url-pattern>/vwsoprouter</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.

The default settings are:

```
<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.

1. Log in to the WebSphere administrative console.
2. Navigate to the Java Virtual Machine settings.

Option	Description
WebSphere Application Server 6.1	Servers → Application Servers → <i>server_name</i> → Java & Process Management → Process Definition → Java Virtual Machine
WebSphere Application Server 7.0	Servers → Server Types → WebSphere application servers → <i>server_name</i> → 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, such as:

**UNIX:** `opt/FileNet/AE`

**Windows:**

```
C:\Progra~1\FileNet\AE
```



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.

**Important:** (Windows only) The path cannot contain a space. You must use 8.3-notation for the install path portion of the full JAAS login entry described above.

If `AE_install_path` is: `C:\Program Files\FileNet\AE`

use: `C:\Progra~1\FileNet\AE`

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 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 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 Performance Tuning Guide, as well as PDF's of the rest of 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 Engine application server and the Application Engine application server. If your Application Engine and Content Engine are on the same WebSphere Application Server, you are not required to configure LTPA.

If you are already using LTPA with your Content Engine application server, you must export only the existing keys and copy the key file to the Application Engine server. Check with your Content Engine administrator.

To configure LTPA:

1. On the Content Engine server, log in to the WebSphere administrative console.
2. Navigate to the LTPA settings page.

Option	Description
WebSphere Application Server 6.1	<ol style="list-style-type: none"> <li>1. Navigate to <b>Security &gt; Secure administration, applications, and infrastructure</b>.</li> <li>2. From the right side of the panel, select <b>Authentication Mechanisms and expiration</b>.</li> </ol>
WebSphere Application Server 7.0	<ol style="list-style-type: none"> <li>1. Navigate to <b>Security &gt; Global security</b>.</li> <li>2. From the right side of the panel, select <b>LTPA</b>.</li> </ol>

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.
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 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 WebSphere Application Server.
10. Copy the key file from the Content 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.

Option	Description
WebSphere Application Server 6.1	<ol style="list-style-type: none"> <li>1. Navigate to <b>Security &gt; Secure administration, applications, and infrastructure</b>.</li> <li>2. From the right side of the panel, select <b>Authentication Mechanisms and expiration</b>.</li> </ol>
WebSphere Application Server 7.0	<ol style="list-style-type: none"> <li>1. Navigate to <b>Security &gt; Global security</b>.</li> <li>2. From the right side of the panel, select <b>LTPA</b>.</li> </ol>

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.
14. Save your changes.

15. In the box for **Cross-cell single sign-on**, type and confirm the **LTPA password** you created for Content Engine.  
For password restrictions, see the WebSphere Application Server documentation. If you have already configured Content 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.

## 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.

To configure stand-alone Lightweight Directory Access Protocol (LDAP):

1. Open the WebSphere administrative console.
2. Navigate to the security settings page.

Option	Description
WebSphere Application Server 6.1	Navigate to <b>Security &gt; Secure administration, applications, and infrastructure</b> .
WebSphere Application Server 7.0	Navigate to <b>Security &gt; Global security</b> .

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.

**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.

To configure Lightweight Directory Access Protocol (LDAP) for federated repositories:

1. Open the WebSphere administrative console.
2. Navigate to the security settings page.

Option	Description
WebSphere Application Server 6.1	Navigate to <b>Security &gt; Secure administration, applications, and infrastructure</b> .
WebSphere Application Server 7.0	Navigate to <b>Security &gt; Global security</b> .

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.

## Configuring Application Engine on WebLogic Server

After you install the Application Engine server, you must configure WebLogic Server to work with Application Engine. You can also configure changes for optional modes like SSO.

“Editing web.xml for SSO (optional)” on page 145

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 WebLogic Server.

“Configuring the application server files” on page 146

As part of the configuration of Application Engine on WebLogic Server, configure the application server files to set up JAAS login information for authentication and memory settings for resource usage.

“Enabling communication between Content Engine and Application Engine (WebLogic Server)” on page 148

To enable communication between Application Engine and Content Engine, you must configure settings on the WebLogic Server.

“Enabling passing user credentials to client applications (WebLogic Server 9.2 only)” on page 149

Some client applications such as WebDAV and Application Integration can require passing user credentials with Application Engine. Enable this communication by editing the config.xml file on the WebLogic Server.

## Editing web.xml for SSO (optional)

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 WebLogic Server.

To edit web.xml for SSO

1. Make a backup copy of web.xml.  
*AE\_install\_path/Workplace/WEB-INF/web.xml*
2. Open web.xml for editing.
3. Set the parameter `perimeterChallengeMode` to true:

```
<init-param>
<param-name>perimeterChallengeMode</param-name>
<param-value>true</param-value>
</init-param>
```

4. 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, then you must set the corresponding `sso*` 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, configure the `<init-param>` parameters as follows:

### **ssoProxyContextPath**

Set the value to the context path of the SSO proxy host URL. This value 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 value:

```
<param-name>ssoProxyContextPath</param-name>
<param-value>/fn/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 value:

```
<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>
```

5. Save your changes to `web.xml` and close the file.

## **Configuring the application server files**

As part of the configuration of Application Engine on WebLogic Server, configure the application server files to set up JAAS login information for authentication and memory settings for resource usage.

To modify the application server files:

1. Stop the WebLogic Server if it is running.
2. Make a backup copy of the `setDomainEnv` file.

For Windows, back up `setDomainEnv.cmd`.

For UNIX, back up `setDomainEnv.sh`.

3. Edit the `MEM_ARGS` variable.

Adjusting this setting prevents the application server from running out of memory, a condition in which users would not be able to log in to Workplace.

If the `MEM_ARGS` variable does not exist, add it to the startup script.

- For all systems except those using JRockit JAVA.

Append the following to the `MEM_ARGS` variable:

```
-XX:MaxPermSize= size m
```

where *size* is the value, in MB, of the **MaxPermSize**.

Refer to your application server vendor recommendation for Initial and Maximum heap size values. For IBM specific recommendations, see the *IBM FileNet P8 Performance Tuning Guide*.

- For systems using JRockit JAVA.

Append the following to the `MEM_ARGS` variable:

```
-Xgc:gencon
```

4. If your application server uses the IBM JVM, edit the `JAVA_OPTIONS` variable to improve performance.

### **UNIX**

Immediately before the following line in the `setDomainEnv` file:

```
SAVE_JAVA_OPTIONS=$JAVA_OPTIONS
```

insert this line (without a carriage return):

```
JAVA_OPTIONS="$JAVA_OPTIONS -Dprogram.name=$PROGRAMNAME
-Dfilenet.pe.peorb.pool.min=2 -Dfilenet.pe.peorb.pool.max=5"
```



## Windows

Immediately before the following line in the setDomainEnv file  
set SAVE\_JAVA\_OPTIONS=%JAVA\_OPTIONS%

insert this line (no carriage return):

```
set JAVA_OPTIONS=%JAVA_OPTIONS% -Dprogram.name=%PROGNAME%
-Dfilenet.pe.peorb.pool.min=2 -Dfilenet.pe.peorb.pool.max=5
```

### 5. Configure JAAS login.

Add one of the following right after the classpath entry for WebLogic Server.

**Important:** Enter the jaas\_login entry as a single line without line breaks. Do not copy and paste the text from this guide because hidden formatting can cause problems with the entry. Instead, type the entry into the script.

**Tip:** Your path might be slightly different depending on the version of your client installations, or whether you have chosen a custom path for installation. Verify the location of the file before you enter the path.

## UNIX

```
Jaas Login configuration setting
JAAS_LOGIN="${JAAS_LOGIN}" -Djava.security.auth.login.config=
"AE_install_path/CE_API/config/jaas.conf.WebLogic"
```

## AIX

```
Jaas Login configuration setting
JAAS_LOGIN="${JAAS_LOGIN}" -Djava.security.auth.login.config=
"AE_install_path/CE_API/config/jaas.conf.WebLogic"
JAAS_LOGIN="${JAAS_LOGIN}"
-Dlogin.configuration.provider=com.ibm.security.auth.login.ConfigFile
```

## Windows

```
@REM Jaas Login configuration setting
set JAAS_LOGIN=%JAAS_LOGIN% -Djava.security.auth.login.config=
"AE_install_path\CE_API\config\jaas.conf.WebLogic"
```

### 6. Make a backup copy of the application server startup script.

For Windows, back up startWebLogic.cmd.

For UNIX, back up startWebLogic.sh

If you are not using a WebLogic domain, back up these files:

For Windows, back up startWLS.cmd

For UNIX, back up startWLS.sh.

### 7. Add the %JAAS\_LOGIN% section to the application server startup script as indicated in the following examples.

#### UNIX - in the WLS\_REDIRECT\_LOG settings

```
${JAVA_HOME}/bin/java ${JAVA_VM} -version

if ["${WLS_REDIRECT_LOG}" = ""] ; then
echo "Starting WLS with line:"
echo "${JAVA_HOME}/bin/java ${JAVA_VM} ${MEM_ARGS} ${JAVA_OPTIONS}
-Dweblogic.Name=${SERVER_
NAME} -Djava.security.policy=${WL_HOME}/server/lib/weblogic.policy
${PROXY_SETTINGS} ${SERVER_CLASS
}"
${JAVA_HOME}/bin/java ${JAVA_VM} ${MEM_ARGS} ${JAVA_OPTIONS}
${JAAS_LOGIN} -Dweblogic.Name=${SERVER_NAME}
-Djava.security.policy=${WL_HOME}/server/lib/weblogic.policy
${PROXY_SETTINGS} ${SERVER_
CLASS}
else
```

```

echo "Redirecting output from WLS window to ${WLS_REDIRECT_LOG}"
${JAVA_HOME}/bin/java ${JAVA_VM} ${MEM_ARGS} ${JAVA_OPTIONS}
${JAAS_LOGIN} -Dweblogic.Name=${SERVER_NAME}
-Djava.security.policy=${WL_HOME}/server/lib/weblogic.policy
${PROXY_SETTINGS} ${SERVER_CLASS} >"${WLS_REDIRECT_LOG}" 2>&1
fi

```

### Windows - in the WLS\_REDIRECT\_LOG settings

```

If "%WLS_REDIRECT_LOG%"==" "(
echo Starting WLS with line:
echo %JAVA_HOME%\bin\java %JAVA_VM% %MEM_ARGS% %JAVA_OPTIONS%
%JAAS_LOGIN% -Dweblogic.Name=%SERVER_NAME%
-Djava.security.policy=%WL_HOME%\server\lib\weblogic.policy
%PROXY_SETTINGS% %SERVER_CLASS% %JAVA_HOME%\bin\java %JAVA_VM%
%MEM_ARGS% %JAVA_OPTIONS% %JAAS_LOGIN%
-Dweblogic.Name=%SERVER_NAME%
-Dweblogic.management.username=%WLS_USER%
-Dweblogic.management.password=%WLS_PW%
-Djava.security.policy=%WL_HOME%\server\lib\weblogic.policy
%PROXY_SETTINGS% %SERVER_CLASS%
) else (
echo Redirecting output from WLS window to %WLS_REDIRECT_LOG%
%JAVA_HOME%\bin\java %JAVA_VM% %MEM_ARGS% %JAVA_OPTIONS%
%JAAS_LOGIN% -Dweblogic.Name=%SERVER_NAME%
-Dweblogic.management.username=%WLS_USER%
-Dweblogic.management.password=%WLS_PW%
-Djava.security.policy=%WL_HOME%\server\lib\weblogic.policy
%PROXY_SETTINGS% %SERVER_CLASS% >"%WLS_REDIRECT_LOG%" 2>&1
)

```

8. Save and close the application server startup script.

### Related information



Product documentation for IBM FileNet P8 Platform

Download the IBM FileNet P8 Performance Tuning Guide, as well as PDF's of the rest of the IBM FileNet P8 Platform documentation.

## Enabling communication between Content Engine and Application Engine (WebLogic Server)

To enable communication between Application Engine and Content Engine, you must configure settings on the WebLogic Server.

To configure Application Engine:

1. (If you selected Container-Managed Authentication during the installation) Enable trust between WebLogic domains for the Content Engine domain and the Application Engine domain.  
Do the following on both the Content Engine application server and the Application Engine application server.
  - a. In the WebLogic Administration Console, in the security settings, enter a password for the domain. You must enter the same password for both the Content Engine domain and Application Engine domain.
  - b. Save your changes.
  - c. Restart the server if needed.
  - d. Repeat this procedure in each domain for which you want to enable trust.
2. (If you selected Container-Managed Authentication during the installation) Configure LDAP settings on Application Engine to exactly match the Content Engine settings.

- a. See your Content Engine installation worksheet items and the Administration Console settings for Compatibility Security > Realms for Authentication Provider, users, and groups on Content Engine. Configure the LDAP provider to exactly match the settings from the Content Engine server:
    - Group Base DN
    - User Name Attribute
    - Port
    - User Base DN
    - Principal
    - Credential
    - Confirm Credential
    - Host
    - User From Name Filter
    - Group From Name Filter
  - b. Restart WebLogic.
3. Set permissions for the user running the application server.

If the user that will be running the application server is different from the user that installed Application Engine, you must give the user read/write permissions on the folder where you installed Application Engine (*AE\_install\_path*).

### Enabling passing user credentials to client applications (WebLogic Server 9.2 only)

Some client applications such as WebDAV and Application Integration can require passing user credentials with Application Engine. Enable this communication by editing the `config.xml` file on the WebLogic Server.

**Important:** If you do not change `config.xml`, then users are prompted to enter their user name and password to complete any client operations, such as adding a document.

To enable passing user credentials:

1. Stop the WebLogic server.
2. Make a backup copy of `config.xml` located in deployment directory.

For example: `BEA_home/bea/user_projects/domains/domain_name/config/config.xml`
3. Edit `config.xml`.

**Important:** The `enforce-valid-basic-auth-credentials` entry must be entered as a single line without line breaks.

- a. Locate the `<security-configuration>` section and add the following line to the end of the section, just before the `</security-configuration>` tag:

```
<enforce-valid-basic-auth-credentials>>false
</enforce-valid-basic-auth-credentials>
```
  - b. Save your changes to `config.xml` and close the file.
4. Restart WebLogic.

## Configuring Application Engine on JBoss Application Server

After you install the Application Engine server, you must configure JBoss Application Server to work with Application Engine. You can also configure changes for optional modes like SSO.

To configure JBoss Application Server for Application Engine:

1. Stop JBoss Application Server if it is running.
2. Make a backup copy of the `run.conf` file and the startup script, depending on your platform:

Option	Description
UNIX	<code>run.sh</code>
Windows	<code>run.bat</code>

3. Edit the `run.conf` file Java settings.
  - a. Add a line to specify the path to the JDK provided by JBoss Application Server, as shown in the following example (Windows):

```
set JAVA_HOME=C:\Program Files\Java\jdk1.5.0_06
```

If your JDK is different from version 1.5.0, substitute your version for the one listed.
  - b. Update the `JAVA_OPTS` memory settings.

Adjusting this setting prevents the application server from running out of memory, a condition in which users would not be able to log in to Workplace.

In the `JAVA_OPTS` line, change the `-Xms` and `-Xmx` values for your configuration.

Example (Windows): `set JAVA_OPTS=%JAVA_OPTS% -Xms 128m -Xmx 512 m`

See your application server vendor recommendation for Initial and Maximum heap size values. For IBM specific recommendations, see the *IBM FileNet P8 Performance Tuning Guide*.
  - c. (Sun JVM users only) Set the value of `MaxPermSize` in `JAVA_OPTS` to 128m, as follows:

```
UNIX
JAVA_OPTS=%JAVA_OPTS% -Xms128m -Xmx512m -XX:MaxPermSize=128m
Windows
set JAVA_OPTS=%JAVA_OPTS% -Xms128m -Xmx512m -XX:MaxPermSize=128m
```

This increased value prevents out of memory errors that can stop JBoss Application Server.
  - d. If your application server uses the IBM JVM, edit the `JAVA_OPTS` variable in the `run.conf` file immediately after the line in the previous substep. This `JAVA_OPTS` edit improves performance.

**UNIX** Find the following line in the `run.conf` file:

```
JAVA_OPTS="$JAVA_OPTS
```

and change it to this (without a carriage return):

```
JAVA_OPTS="$JAVA_OPTS -Dfilenet.pe.peorb.pool.min=2
-Dfilenet.pe.peorb.pool.max=5"
```

**Windows**

Find the following line in the `run.conf` file:

```
set JAVA_OPTS=%JAVA_OPTS%
```

and change it to this (without a carriage return):

```
set JAVA_OPTS=%JAVA_OPTS% -Dfilenet.pe.peorb.pool.min=2
-Dfilenet.pe.peorb.pool.max=5
```

e. Save your edits and close the file.

#### 4. Configure JAAS login.

Add one of the following right after the "\$JAVA" \$JAVA\_OPTS (UNIX) or "%JAVA%" %JAVA\_OPTS (Windows) entry in the run.sh file for UNIX or the run.bat for Windows.

**Important:** Enter the jaas\_login entry as a single line without line breaks. Do not copy and paste the text from this guide because hidden formatting can cause problems with the entry. Instead, type the entry into the script.

Your path might be slightly different depending on the version of your client installations, or whether you have chosen a custom path for installation. Verify the location of the file before you enter the path.

#### UNIX

```
"$JAVA" $JAVA_OPTS
-Djava.security.auth.login.config=
"/opt/FileNet/AE/CE_API/config/jaas.conf.JBoss"
-Djava.endorsed.dirs=$JBOSS_ENDORSED_DIRS" -classpath
"$JBOSS_CLASSPATH" org.jboss.Main $@
```

#### Windows

```
"%JAVA%" %JAVA_OPTS%
-Djava.security.auth.login.config=C:\Program
Files\FileNet\AE\CE_API\config\jaas.conf.JBoss"
-Djava.endorsed.dirs=%JBOSS_ENDORSED_DIRS%" -classpath
"%JBOSS_CLASSPATH%" org.jboss.Main %*
```

5. Save and close the run.sh or run.bat file.

6. Configure LDAP settings on Application Engine to exactly match the Content Engine settings.

a. On the Application Engine server, open login-config.xml, located in *JBoss\_home/server/server\_name/conf*, for editing.

b. Set the <application-policy name="FileNet"> entry identical to the corresponding entry in the login-config.xml file on the Content Engine server.

c. Set the <application-policy name="FileNetP8Engine"> entry identical to the corresponding entry in the login-config.xml file on the Content Engine server.

d. Copy the new <application-policy name="FileNetP8Engine"> entry, and paste the copied entry directly before the entry you copied (<application-policy name="FileNetP8Engine">).

e. Change the first instance of the <application-policy name="FileNetP8Engine"> to <application-policy name="FileNetP8">.

f. Move all the FileNet-related <application-policy name=> entries above the <application-policy name="other"> entry.

g. Save changes to the login-config.xml file on the Application Engine server.

h. Restart JBoss Application Server.

7. Set permissions for the user running the application server.

On Windows, the following is only required for NTFS formatted partitions.

If the user that runs the application server is different from the user that installed Application Engine, you must give the user read and write permissions on the folder where you installed Application Engine (*AE\_install\_path*).

8. (Optional) Disable JBoss Application Server logging.

In development mode, JBoss Application Server creates many HTTP Access, "INFO", "DEBUG" and "TRACE" log messages. This can cause unexpected behavior in the deployed IBM FileNet software. You can limit this type of excessive JBoss Application Server logging.

When logging is disabled, error messages still display in the JBoss Application Server console.

- a. Open the `log4j.xml` file (*JBoss\_home/server/server\_name/conf/log4j.xml*) for editing.
- b. Change all threshold values and priority values from "INFO", "DEBUG", or "TRACE" to "ERROR".
- c. Delete or comment out the "Preserve messages in a local file" to turn off the server log.
- d. To turn off HTTP access logging, open `jboss-service.xml` with a text editor and delete or comment out the "Access logger" section.

Location of `jboss-service.xml`:

*JBoss\_Home/server/server\_name/deploy/jbossweb-tomcat55.sar/META-INF*

- e. Open `web.xml` for editing and change the `logVerbosityLevel` to "FATAL".

Location of `web.xml`:

*JBoss\_Home/server/server\_name/deploy/jbossweb-tomcat55.sar/conf*

- f. Restart the JBoss Application Server server.

---

## 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.

“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 WebLogic Server” on page 156

After you install and configure Application Engine, you must deploy your client application, Workplace, on your WebLogic Server. You might be required to re-create the WAR or WAR and EAR files before you deploy.

“Deploying Application Engine on JBoss Application Server” on page 158

After you install and configure Application Engine, you must deploy your client application, Workplace, on your JBoss 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.

“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 6.1)” on page 154  
Deploy Application Engine as an application in the WebSphere 6.1 administrative console. You can specify the context root for the application URL during the deployment.

“Deploying the application (WebSphere Application Server 7.0)” on page 155  
To use Workplace as a web application, you must deploy it as an application in the WebSphere 7.0 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
UNIX	AE_install_path/deploy/create_app_engine_war.sh
Windows	AE_install_path\deploy\create_app_engine_war.bat

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
UNIX	AE_install_path/deploy/create_app_engine_ear.sh
Windows	AE_install_path\deploy\create_app_engine_ear.bat



## Deploying the application (WebSphere Application Server 6.1)

Deploy Application Engine as an application in the WebSphere 6.1 administrative console. You can specify the context root for the application URL during the deployment.

To deploy Application Engine:

1. Log on to the WebSphere administrative console.
2. Navigate to **Applications > 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 that you log in to by 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 dialog boxes for installing a new application by 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 application class loader first**.
10. Click **Apply**.
11. Click **Workplace > Manage Modules**.
12. Click **Workplace**.
13. Change the **Class loader order** to **Classes loaded with application class loader first**.

**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**. Verify that the **All Authenticated** column is checked for the "All Authenticated" role.
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.

### Deploying the application (WebSphere Application Server 7.0)

To use Workplace as a web application, you must deploy it as an application in the WebSphere 7.0 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 in 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.

## Deploying Application Engine on WebLogic Server

After you install and configure Application Engine, you must deploy your client application, Workplace, on your WebLogic Server. You might be required to re-create the WAR or WAR and EAR files before you deploy.

### “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 Application Engine” on page 157

To use Workplace as a web application, you must deploy it as an application in the WebLogic Server Administration 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
UNIX	<i>AE_install_path</i> /deploy/ create_app_engine_war.sh
Windows	<i>AE_install_path</i> \deploy\ create_app_engine_war.bat

- (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 by default creates 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.

- (For EAR file deployments only) re-create the `app_engine.ear` file by running the script for your platform.

Option	Description
UNIX	<i>AE_install_path</i> /deploy/ create_app_engine_ear.sh
Windows	<i>AE_install_path</i> \deploy\ create_app_engine_ear.bat

## Deploying Application Engine

To use Workplace as a web application, you must deploy it as an application in the WebLogic Server Administration Console. You can specify the context root for the application URL during the deployment.

- From the WebLogic Server Administration Console, navigate to the domain you initially created for the Application Engine.
- Prepare the WebLogic Server Administration Console to deploy the application.
- Choose whether to deploy from an exploded folder (*AE\_install\_path*) or from the WAR or EAR file (default: `app_engine.war` or `app_engine.ear` in *AE\_install\_path*/deploy).
- Accept the defaults for the deployment, except for the name for the deployment. Use "Workplace" instead of "appengine".
- Finish the deployment, and save and activate your changes.

**Tip:** To verify that the deployment was successful, expand **Web Applications**. The web application Workplace is listed.

**Tip:** To troubleshoot the deployment, check the following log:

```
WLS_install_path/user_projects/domains/domain_name/servers/server_name/logs/server_name.log
```

- After deployment is complete, start Workplace (or your custom application name) in the WebLogic Server Administration Console.

## Deploying Application Engine on JBoss Application Server

After you install and configure Application Engine, you must deploy your client application, Workplace, on your JBoss Application Server. You might be required to re-create the WAR or WAR and EAR files before you deploy.

“Recreating the WAR or EAR file”

Any time that you make changes to files in the /Workplace directory, such as changes to web.xml for container-managed authentication, SSO support, or any other edits, you must recreate the WAR or EAR file and redeploy your changes.

“Deploying and starting Application Engine” on page 159

After you install and configure Application Engine, you must deploy your client application, Workplace, on your JBoss Application Server.

### Recreating the WAR or EAR file

Any time that you make changes to files in the /Workplace directory, such as changes to web.xml for container-managed authentication, SSO support, or any other edits, you must recreate the WAR or EAR file and redeploy your changes.

**Remember:** Before recreating the EAR file, you must first recreate the WAR file.

To recreate the WAR or EAR files:

1. Verify that all modified /Workplace directory files have been saved.
2. Recreate the app\_engine.war file by running the script for your platform.

Option	Description
UNIX	<i>AE_install_path</i> /deploy/ create_app_engine_war.sh
Windows	<i>AE_install_path</i> \deploy\ create_app_engine_war.bat

3. (For WAR file deployment) Rename the newly recreated 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 will generate the following context root: `http://server_name:port#/app_engine`. Renaming the WAR file Workplace.war will generate 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 will by default create a file with the name app\_engine.war.

**Important:** Do not rename the WAR file if you are using the WAR file to recreate the EAR file for deployment.

4. (For EAR file deployments only) Recreate the app\_engine.ear file by running the script for your platform.

Option	Description
UNIX	<i>AE_install_path</i> /deploy/ create_app_engine_ear.sh
Windows	<i>AE_install_path</i> \deploy\ create_app_engine_ear.bat

## Deploying and starting Application Engine

After you install and configure Application Engine, you must deploy your client application, Workplace, on your JBoss Application Server.

1. Stop the JBoss Application Server, if it is running.
2. Deploy the Workplace application: To deploy from exploded directory
  - a. On the JBoss Application Server, copy the /Workplace folder from:  
*AE\_install\_path*  
to:  
*JBOSS\_home/server/servername/deploy/*
  - b. Append the extension *.war* to the Workplace folder:  
*JBOSS\_home/server/servername/deploy/Workplace.war*  
To deploy from a WAR file  
On the JBoss Application Server, copy the *app\_engine.war* file from:  
*AE\_install\_path/deploy*  
to:  
*JBOSS\_home/server/servername/deploy/*  
To deploy from an EAR file  
On the JBoss Application Server, copy the *app\_engine.ear* file from:  
*AE\_install\_path/deploy*  
to:  
*JBOSS\_home/server/servername/deploy/*
3. Set permissions for the user running the application server.  
If the user that will be running the application server is different from the user that installed Application Engine, you must give the user read/write permissions on the following folders:  
*JBOSS\_home/server/default/deploy/app\_engine.war/ .ear*  
*AE\_install\_path*  
For Windows this is only required for NTFS formatted partitions.
4. Start the JBoss Application Server.
5. Verify that the application deployed successfully.  
Verify that the *server.log* file located in *JBOSS\_home/server/servername/log* lists deployment of the WAR or EAR file you used.

---

## 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” on page 160

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 162

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 163  
To allow users to create workflow 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 163

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 using Workplace Site Preferences. For more information, see the IBM FileNet P8 help topic **User Help** → **Actions, preferences, and tools** → **Site preferences**.

### 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**. 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 **User Help** → **Actions, preferences, and tools** → **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 171 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 (if installed). 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 documentation server URL in the **Documentation server** field.

The format of the URL depends on the documentation package you use:

Table 14. Documentation URLs

FileNet P8 Documentation package	URL
Online information center at www.ibm.com	http://publib.boulder.ibm.com/infocenter/p8docs/v4r5m1/index.jsp
Installed Eclipse-based information center	http://yourdocserver:port#/p8docs/index.jsp
Installed non-Eclipse-based documentation package	http://yourdocserver:port#/ecm_help/_start_here.htm

If no documentation URL is specified, the Workplace Help link will default to http://localhost.

- d. Enter the ISRA Interface Servlet URL.  
For more information, see “Enabling Application Engine to use ISRA” on page 191.
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 **User Help** → **Actions, preferences, and tools** → **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. For more information, see the *IBM FileNet P8 High Availability Technical Notice*.

## 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 IBM FileNet P8 help topic *User Help > Actions, preferences, and tools > 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, see the IBM FileNet P8 help topic **System Administration > Content Engine Administration > Content Engine Wizard Help > Security Script**.

For more information about the `workplacescript.xml` file and how roles are defined in the Enterprise Manager, see the IBM FileNet P8 help topic **System Administration > Content Engine Administration > 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 **System Administration > Application Engine > Administration > Key configuration files and logs > bootstrap.properties**.

### Related information

 [IBM FileNet P8 High Availability Technical Notice](#)

Install and initially configure IBM FileNet P8 products on a high availability system.



---

## Configuration and startup tasks

After you install the IBM FileNet P8 components, there are some additional steps to configure the IBM FileNet P8 system. After you configure the IBM FileNet P8 components, familiarize yourself with IBM FileNet P8 system startup and shutdown procedures. See the **System Administration** → **Enterprise-wide Administration** → **Startup and Shutdown** help topic.

“Creating a Process Engine isolated region”

Process Engine clients communicate to isolated regions in the database and to the Process Engine server by using a connection point. Each connection point is associated with an isolated region. In this task you will create an isolated region.

“Creating a Process Engine Connection Point” on page 166

A connection point identifies a specific isolated region of the workflow database, and gives it a name that workflow-related applications use to access the region. Follow these procedures to create a connection point.

“Configuring the Process Engine connection point for Application Engine” on page 167

Before users can access Process Engine tasks and work items from Workplace, you must configure the connection point on the Application Engine.

“Setting up Content Engine and client transport SSL security” on page 168

Configuring SSL enables secure communications between the Content Engine and the directory service, as well as between Content Engine clients and the Content Engine server. In addition, setting up Content Engine SSL provides secure authentication for Process Engine.

“Setting up Application Engine SSL security” on page 171

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 174

Once you have completed the installation tasks, your core IBM FileNet P8 system is operational. You can do the recommended additional configuration tasks to prepare the system for general use.

---

### Creating a Process Engine isolated region

Process Engine clients communicate to isolated regions in the database and to the Process Engine server by using a connection point. Each connection point is associated with an isolated region. In this task you will create an isolated region.

In “Configuring the Process Engine connection point for Application Engine” on page 167 you will define a connection point to this isolated region.

To create a Process Engine isolated region:

1. Start Enterprise Manager by double-clicking the FileNet Enterprise Manager SnapIn on the desktop, or by navigating to **Start > All Programs > FileNet P8 Platform > FileNet Enterprise Manager Administration Tool**. Log on as a GCD administrator.
2. Connect to the FileNet P8 domain that you created previously.
3. Right-click **PE Region ids > New PE Region ids**.

4. On the Specify a Site screen, click **Next** to select a site named *initial site* .
5. Enter the DNS name for the Process Engine server. This is the network name from the installation worksheet.
6. Enter the region ID.
7. Modify the communication port if needed. This communication port must match the password that was entered in the Process Task Manager for the communication port in “Configuring Process Task Manager” on page 119.
8. Click **Next**.
9. Enter the password for the isolated region. This password must match the password entered in the Process Task Manager for the isolated region in “Configuring Process Task Manager” on page 119.
10. Click **OK** on the Confirmation Window.
11. Click **Finish** to finish creating a new isolated region for Process Engine.

#### Related tasks

“Establishing the FileNet P8 domain and Global Configuration Data (GCD)” on page 69

With Content Engine installed and deployed, you must use IBM FileNet Enterprise Manager to create a FileNet P8 domain. You can also use Enterprise Manager to set a URL to the FileNet P8 online help if you did not specify the location when you ran the Content Engine installation program.

---

## Creating a Process Engine Connection Point

A connection point identifies a specific isolated region of the workflow database, and gives it a name that workflow-related applications use to access the region. Follow these procedures to create a connection point.

To create a Process Engine connection point:

1. Start Enterprise Manager by double-clicking the FileNet Enterprise Manager SnapIn on the desktop, or by navigating to **Start > All Programs > FileNet P8 Platform > Enterprise Manager SnapIn**. Log in as a GCD administrator.
2. Connect to the FileNet P8 domain that you created previously.
3. Right-click **PE Connection Points** → **New PE Connection Points**.
4. Enter a Process Engine Connection Point name and click **Next**.  
Process Engine Connection Point names must not contain whitespace characters.
5. Choose the region which is created in “Creating a Process Engine isolated region” on page 165, and click **Next**.
6. Click **Finish** to finish creating the Connection Point.
7. Click **OK**.

### Related tasks

“Establishing the FileNet P8 domain and Global Configuration Data (GCD)” on page 69

With Content Engine installed and deployed, you must use IBM FileNet Enterprise Manager to create a FileNet P8 domain. You can also use Enterprise Manager to set a URL to the FileNet P8 online help if you did not specify the location when you ran the Content Engine installation program.

---

## Configuring the Process Engine connection point for Application Engine

Before users can access Process Engine tasks and work items from Workplace, you must configure the connection point on the Application Engine.

Make sure that you have already created a Process Engine isolated region and a Process Engine connection point and that the Process 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.
  - 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 enter the following settings:

    - Clear the **Internet Explorer** option.
    - If you will be using Netscape 6.0, select the **Netscape** 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 Engine and client transport SSL security

Configuring SSL enables secure communications between the Content Engine and the directory service, as well as between Content Engine clients and the Content Engine server. In addition, setting up Content Engine SSL provides secure authentication for Process Engine.

**Important:** IBM strongly recommends enabling SSL for the Content Engine and Process 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. In the IBM FileNet P8 4.5 release, Kerberos authentication is available only for the Content 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 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 Engine web service is used:
  - By all clients of the Content Engine version 4.5.1 .NET API
  - By all clients of the Content Engine version 4.5.1 COM Compatibility API (CCL)
  - By the Enterprise Manager tool
  - By the Content Engine version 3.5.2 to 4.5.1 Upgrade tool
  - By the Process Engine, when making calls to the Content Engine to retrieve user and group information
  - By the Component Manager, running on the Application Engine, which is an integral component for BPM Process Orchestration framework
  - By customer and 3rd party tools written against the Content Engine version 3.5 web service API, including Altien Document Manager and the Sharepoint integration done by Vorsite.
- Certain Java applications (written against the Content Engine version 3.5 Java API or the Content Engine 4.5 Java API) might use the Content 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 Engine in the 4.5.1 release.
- The Process Engine web service is used by customer and independent software vendor applications to write runtime applications (typically step processor applications) against the Process Engine. The Process Engine Java API does not make use of the Process Engine web service.

“Enabling SSL for Content Engine” on page 169

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 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 171

Use the Enterprise Manager interface to enable SSL between Enterprise Manager and the directory service.

## Enabling SSL for Content 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 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 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 Engine server, add the CA certificate to the application server keystore, if it does not already contain it.
4. On the Content 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. Use Enterprise Manager to enable SSL for Content Engine and set the port number to match the SSL port on the directory server.
6. Obtain another server and CA certificate for the Content Engine.
7. Create a custom identity keystore on the Content Engine server, and add the server certificate to the custom keystore.
8. 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.
Oracle WebLogic Server	Set up a custom identity keystore. In the left pane of the WebLogic Administration Console, navigate to <i>DomainName</i> > Servers > <i>ServerName</i> . In the right pane, select Keystores and SSL and specify the keystore information.
JBoss Application Server	See your application server documentation.

**Important:** (WebLogic only) The name in your certificate must match the host name specified in your WebLogic application server. If the name in the certificate is fully qualified (for example, Host1.filenet.com), the same fully qualified host name must appear in the Host field (**WebLogic** → **Authentication Provider** → **Active Directory tab** → **Host field**).

9. Configure clients to use a particular URL for connecting to Content Engine based on the application server type and the client transport (protocol) type. The following table provides the default ports and sample URLs:

Protocol	SSL	Default Port	App Server	Sample URL
HTTP	no	9080	WebSphere Application Server	http://mycorp.com:9080/wsi/FNCEWS40MTOM/
HTTPS	yes	9443	WebSphere Application Server	https://mycorp.com:9443/wsi/FNCEWS40MTOM/
IIOP	no	2809	WebSphere Application Server	iiop://mycorp.com:2809/FileNetEngine
IIOP	yes	2809	WebSphere Application Server	iiop://mycorp.com:2809/FileNetEngine (default)
While the default port for IIOP with SSL is port 9403, use port 2809. The web application server resolves the SSL port number correctly.				
HTTP	no	7001	WebLogic	http://mycorp.com:7001/wsi/FNCEWS40MTOM/
HTTPS	yes	7002	WebLogic	https://mycorp.com:7002/wsi/FNCEWS40MTOM/
T3 (IIOP)	no	7001	WebLogic	t3://mycorp.com:7001/FileNet/Engine
T3S (IIOP)	yes	7002	WebLogic	t3s://mycorp.com:7002/FileNet/Engine
HTTP	no	8080	JBoss	http://mycorp.com:8080/wsi/FNCEWS40MTOM/
HTTPS	yes	8443	JBoss	https://mycorp.com:8443/wsi/FNCEWS40MTOM/

Protocol	SSL	Default Port	App Server	Sample URL
JNP	no	1099	JBoss	jnp://mycorp.com:1099/ FileNet/Engine

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 Engine client.

## 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.

## 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” on page 172

To set up full SSL support, enable SSL on the preferred application server.

“Setting up SSL redirect on a single Application Engine server” on page 172

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 173

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 174

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 **User Help** → **Using Workplace** → **Basics** → **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 *User Help > Actions, preferences, and tools > 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 *User Help > Actions, preferences, and tools > 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. See "Setup WebLogic clusters" or "Setup WebSphere clones" in the *IBM FileNet P8 High Availability Technical Notice* for specific instructions.

**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 **User Help** → **Actions, preferences, and tools** → **Site preferences** → **Bootstrap Preferences** → **User token settings**.

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 **User Help** → **Actions, preferences, and tools** → **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 **User Help** → **Actions, preferences, and tools** → **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.

#### Related information

 IBM FileNet P8 High Availability Technical Notice  
Install and initially configure IBM FileNet P8 products on a high availability system.

## 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 **User Help** → **Using Workplace** → **Basics** → **Use Java applets** to resolve this issue.

---

## Performing additional configuration tasks

Once you have completed the installation tasks, your core IBM 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 IBM FileNet P8 help. The documentation URL varies depending on the documentation package you use.

*Table 15. Documentation URLs*

FileNet P8 Documentation package	URL
Online information center at <code>www.ibm.com</code>	<code>http://publib.boulder.ibm.com/infocenter/p8docs/v4r5m1/index.jsp</code>
Installed <code>ecm_help</code> documentation package	<code>http://yourdocserver:port#/ecm_help/_start_here.htm</code>


- 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 **System Administration** → **Application Engine Administration** → **Key configuration files and logs** → **content\_redir.properties file**.
- Set site preferences for the Workplace application. See **User Help** → **Actions, preferences, and tools** → **Site preferences**.



- Design searches and/or search templates for Workplace users. See **User Help** → **Actions, preferences, and tools** → **Search Designer** → **About Search Designer**.
- Design publishing templates for Workplace users. See **User Help** → **Actions, preferences, and tools** → **Tools** → **Publishing Designer** → **About Publishing Designer**.
- Configure security for publishing. See **User Help** → **Actions, preferences, and tools** → **Tools** → **Publishing Designer** → **Security** → **Specify publication document security**.
- Configure automatic workflow launch. See **System Administration** → **Content Engine Administration** → **Events and subscriptions** → **Concepts: workflow subscriptions**.
- Create and configure the object stores that will contain business objects, folders, documents, workflow definitions, searches, and other objects. See **System Administration** → **Content Engine Administration** → **Object stores** → **How to... → Create object store**.
- Define document classes and folders and set security for each class. See **System Administration** → **Content Engine Administration** → **Classes** → **Concepts**.
- Review and, if necessary, edit the security of the network shared folders containing any file stores created for the object store. See **System Administration** → **Content Engine Administration** → **Content storage** → **File storage areas** .
- Configure Process Engine for automatic startup. See **System Administration** → **Enterprise-wide Administration** → **Process Task Manager** → **Process Engine** → **Process Service** → **Start and stop Process Service** → **Configure the Process Service for automatic startup (Windows)**.
- Configure e-mail notification. See **System Administration** → **Process Engine Administration** → **Workflow administration tasks** → **Coordinating workflow design** → **Email notification**.
- Set Process Engine runtime options. See **User Help** → **Integrating workflow** → **Process Configuration Console** → **VWServices** → **View or modify VWService properties** → **Set runtime options**.
- Set the default date/time mask for the Process Service. See **Process Engine** → **Process Task Manager** → **Process Service** → **Configuring Process Service** → **General properties**.
- Create content cache area. See **System Administration** → **Content Engine Administration** → **Content storage** → **Content cache areas** → **How to... → Create content cache**.
- Create additional authentication realms. See **System Administration** → **Enterprise-wide Administration** → **FileNet P8 Security** → **How to** → **Configure for multiple realms**.
- Define additional isolated regions. See **User Help** → **Integrating workflow** → **Process Configuration Console** → **Isolated regions**.
- For each isolated region:
  - Define workflows. See **User Help** → **Integrating workflow** → **Process Designer**.
  - Configure event logging options. See **User Help** → **Integrating workflow** → **Process Configuration Console** → **Isolated regions** → **View or modify isolated region properties** → **Configure event logging options**.
  - Configure step processors. See **User Help** → **Integrating workflow** → **Process Configuration Console** → **Isolated regions** → **View or modify isolated region properties** → **Configure custom step processors**.

- Define and configure work queues. See **User Help** → **Integrating workflow** → **Process Configuration Console** → **Queues** → **Configuring work queues**.
- Define and configure component queues. See **User Help** → **Integrating workflow** → **Process Configuration Console** → **Queues** → **Configuring component queues**.
- Define and configure workflow rosters. See **User Help** → **Integrating workflow** → **Process Configuration Console** → **Queues** → **Rosters**.

#### **Related information**

 Product documentation for IBM FileNet P8 Platform  
Download the IBM FileNet P8 Non-English Support Guide, as well as PDF's of the rest of the IBM FileNet P8 Platform documentation.

---

## Optional installation tasks

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

“Installing and Configuring IBM FileNet P8 publishing components” on page 178

For publishing capabilities, install the IBM FileNet Rendition Engine.

“Enabling the Process Engine Component Integrator” on page 178

By using the Component Integrator functionality included in the IBM FileNet P8 Platform, a step in a workflow can access properties of documents, folders, and other objects in an object store. Using this functionality requires configuration on both Application Engine and Process Engine servers.

“Installing an additional instance of Enterprise Manager” on page 180

You can install an instance of Enterprise Manager in addition to the one that you already installed.

“Creating additional file storage areas” on page 181

Perform this task to create additional file storage areas for existing object stores. To create additional fixed storage areas, navigate instead to the IBM FileNet P8 help topic **System Administration** → **Content Engine Administration** → **Content storage** → **Fixed storage areas**.

“Installing IBM FileNet Deployment Manager” on page 182

IBM FileNet Deployment Manager works with Enterprise Manager to deploy test systems into full production. You can install the IBM FileNet Deployment Manager interactively or silently on a Windows machine.

“Installing Application Integration” on page 184

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 Workplace File Tracker” on page 186

If you want to use the file tracking feature without installing Application Integration, you can install Workplace File Tracker. Complete the installation on each machine that will use Workplace File Tracker.

“Deploying multiple Application Engine instances” on page 189

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 191

Image Services Resource Adaptor (ISRA) is a J2EE connector to the IBM FileNet Image Services libraries. Using ISRA, Workplace users can view 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 195

Content Engine, Application Engine, and Process Engine install, by default, the necessary software required for the System Manager performance component. To use System Manager, enable associated components and install IBM System Dashboard for Enterprise Content Management to perform related configuration procedures to enable System Manager.

“Modifying an Autonomy K2 server configuration” on page 195

You can add Autonomy K2 servers or move existing servers to new hardware.

“Installing the COM compatibility layer (CCL)” on page 203  
The option to install the COM compatibility layer is available as part of the IBM FileNet P8 Content Engine installer.

---

## 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 the *IBM FileNet Rendition Engine Installation and Upgrade Guide* at **FileNet P8 Documentation** → **FileNet P8 System Installation** → **Rendition Engine Installation and Upgrade**.

---

## Enabling the Process Engine Component Integrator

By using the Component Integrator functionality included in the IBM FileNet P8 Platform, a step in a workflow can access properties of documents, folders, and other objects in an object store. Using this functionality requires configuration on both Application Engine and Process Engine servers.

As a post-installation task, you must define workflows that incorporate Content Engine operations in order to use the out-of-the-box Component Integrator functionality. For further details on defining such workflows, see the IBM FileNet P8 help topic **Steps** → **Component Steps** → **General Properties** → **Using Content Engine (CE) operations in a workflow**.

After the software is installed, users can extend the out-of-the-box Component Integrator functionality so that a workflow step can interact with an external entity such as a Java object or Java Messaging Service (JMS) messaging system. For further information, see the IBM FileNet P8 help topic **Developing Process Applications** → **Developing Work Performers / Component Integrator Operations**.

To specify the user name and password for the Java adaptor (on an Application Engine server):

1. Sign in to Workplace.  
If you defined the Process Engine Configuration Group on the Security tab of Process Task Manager (when completing “Configuring Process Task Manager” on page 119), you must sign in as a member of either that group or the Process Engine Administrators Group, which was also defined on the Security tab, in order to complete the following steps.
2. In Workplace, click **Admin** and then 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.  
For further information about the JRE download, click **Help** in Process Configuration Console, click **Process Reference** on the help page toolbar, and see the IBM FileNet P8 help topic **Concepts** → **Java Runtime Environment (JRE)**.
3. Select the Isolated Region icon that corresponds to the isolated region that you initialized. For more information, see “Creating a Process Engine isolated region” on page 165.
4. Right-click the **CE\_Operations** component queue and select **Properties** .

- On the Adaptor tab of the displayed dialog box, enter a user name and password that will be used for identification and permissions for both Process Engine and potentially any external systems that will be accessed. By default, the user name and password are set to *Administrator* and *<no password>*, respectively. If you choose to use another user name and password, they must already exist in the directory service.

For additional information about the fields on the Adaptor tab, click the **Help** button. To use the out-of-the-box functionality, it is necessary to modify only the user name and password fields.

- Click **OK** and commit the changes.

“Configuring and starting the Component Manager (on an Application Engine server)”

Configure the Component Manager and start it on an Application Engine.

“Specifying connection between Process Engine and Component Manager (on a Process Engine server)” on page 180

Configure the connection between the Process Engine and the Component Manager using Process Task Manager on the Process Engine.

## Configuring and starting the Component Manager (on an Application Engine server)

Configure the Component Manager and start it on an Application Engine.

- Start Process Task Manager on the Application Engine server by running one of the following command files from the *AE\_install\_path/FileNet/AE/Router* directory, depending on your operating system:.

Option	Description
UNIX	routercmd.sh
Windows	routercmd.bat

If the Registry Port assigned to Component Manager conflicts with the port number required by another application or service running on the Application Engine server, Process Task Manager will not start up as expected and the necessary *vtaskman.xml.sample* will not be automatically created. If this happens, make a copy of the sample *vtaskman.xml.sample* file located on the Process Engine or Application Engine.

- On Process Engine, the file is located in the */fnsw/bin* directory.
- On Application Engine, the file is located in:
  - Drive:\Program Files\FileNet\AE\Router on Windows
  - */opt/FileNet/AE/Router* on UNIX

Open *vtaskman.xml.sample* with a text editor, change the port element value to an available port number, and save the file to *vtaskman.xml* in the same directory.

- In Process Task Manager, select the server name in the left pane.
- Find the Registry Port for the server in the right pane and verify that it is correct.
- Select **Component Managers** in the left pane .
- Enter the Content URI , service username, and service password Content URI to authenticate to the Content Engine server. The Content URI defaults and you can use the default or change the value.
- Right-click and select **New** to select a connection point from the drop down list.

7. Enter or modify the component properties as appropriate. For details, see the **System Administration** → **Enterprise-wide Administration** → **Process Task Manager** → **Component Manager** → **Configure Component Manager** → **General properties**. In an environment configured for single sign-on (SSO), do not use the SSO server name in the URL, even if Process Task Manager displays it by default.
8. Click **Start** on the toolbar.

#### Related concepts

 IBM FileNet P8 ports

For details on how to resolve port number conflicts, see *Plan and Prepare Your Environment for IBM FileNet P8*.

## Specifying connection between Process Engine and Component Manager (on a Process Engine server)

Configure the connection between the Process Engine and the Component Manager using Process Task Manager on the Process Engine.

Configuring this connection is not recommended in a high availability configuration.

1. On the Process Engine server, start Process Task Manager as follows, depending on your operating system:

Option	Description
UNIX	Enter the following command on the command line: <code>vwtaskman</code>
Windows	Select <b>Start</b> > <b>Programs</b> > <b>IBM FileNet P8 Platform</b> > <b>Process Engine</b> > <b>Process Task Manager</b> .

2. Select Process Engine in the left pane (also referred to as the feature pane).
3. In the **Component Manager connection** section, select the **Server Connections** tab.
4. In the **Host** field, enter the host name of the Application Engine server where Component Manager is running.
5. In the **Event Port** field, enter the port that the Component Manager listens to for incoming events. The default is 32773. The port number you enter must match the number you entered when you configured the Component Manager previously.

## Installing an additional instance of Enterprise Manager

You can install an instance of Enterprise Manager in addition to the one that you already installed.

**Important:** Do not install Enterprise Manager version 4.5.1 or the COM Compatibility Clients API on any machine that is running the 3.5 version, at least until the Content Engine 4.5.1 upgrade is complete. Otherwise, you will no longer be able to run Enterprise Manager 3.5 against any remaining 3.5 object stores. You might be required to use Enterprise Manager to prepare for upgrading the 3.5 object stores.

**Remember:** You can install Enterprise Manager only on a Windows machine by using the Windows version of the Content Engine installation media.

To install an additional instance of 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 Engine values, filter by **CE 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 Windows components.

Option	Description
Microsoft Windows XP, Microsoft Windows Server 2003	Microsoft .NET Framework 2.0 and Web Services Enhancements (WSE) 3.0
Content Engine version 4.5.1 Fix Pack 002 or higher with Microsoft Windows Vista, Microsoft Windows Server 2008, or Microsoft Windows 7	Microsoft .NET Framework 3.0 and Windows Communication Foundation (WCF)

4. Access the Content Engine software package.
5. Start the Enterprise Manager installation.

Option	Description
To install interactively	<ol style="list-style-type: none"> <li>1. Run the following command in the software package: P8CE-4.5.1-WIN.exe.</li> <li>2. Complete the installation program wizard.</li> </ol>
To install silently	<ol style="list-style-type: none"> <li>1. Open the CE_silent_install.txt file in the software package for editing.</li> <li>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: <b>DotNetClients,AdminTools</b></li> <li>3. Save your edits.</li> <li>4. Run the following command in the software package on a single line: P8CE-4.5.1-WIN.EXE -f CE_silent_install.txt -i silent</li> </ol>

6. Install any service packs, fix packs, or interim fixes.

---

## Creating additional file storage areas

Perform this task to create additional file storage areas for existing object stores. To create additional fixed storage areas, navigate instead to the IBM FileNet P8 help topic **System Administration → Content Engine Administration → Content storage → Fixed storage areas**.

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



Complete the following procedure for each file storage area you want to create.

1. Prepare a location for the file storage area, as shown in "Prepare storage areas for object stores" in *Plan and Prepare Your Environment for IBM FileNet P8*.
2. 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 Enterprise Manager values for this task, filter by **EM: Create a Storage Area** in the **Installation or Configuration Program** column.

3. Start Enterprise Manager.
4. Select a FileNet P8 domain and log on as an administrator of the object store in which you will create a file storage area.
5. Right-click the **Storage Areas node** and then choose **New Storage Area**.
6. When the Create a Storage Area wizard opens, complete the wizard screens by using the values in your worksheet.

"Verifying the file storage area"

To verify the file storage area, log onto the machine that Content Engine Server is installed and verify that fsa1 contains an XML file named fn\_stakefile.

## Verifying the file storage area

To verify the file storage area, log onto the machine that Content Engine Server is installed and verify that fsa1 contains an XML file named fn\_stakefile.

1. Log on to the machine where the Content Engine Server is installed.
2. List the contents of the fsa1 directory you created or designated when you configured your file server.
3. Verify that fsa1 contains an XML file, named fn\_stakefile, and two subdirectories, content and inbound.

**Important:** On UNIX machines, the content and inbound subdirectories must be in the same file system.

4. Verify that fsa1 has the ownership and access permissions you specified.
5. Assign the new storage area as the default storage location for one of your document classes. See the IBM FileNet P8 help topic **System Administration** → **Content Engine Administration** → **Content storage** → **File storage areas** for more information.

### Related information

 [Configuring a UNIX-based file server](#)

For more information about the fsa1 directory, see the "Configuring a UNIX-based file server" in *Plan and Prepare Your Environment for IBM FileNet P8*.

 [Configuring a Windows-based file server for a Windows client](#)

For more information about the fsa1 directory, see *Plan and Prepare Your Environment for IBM FileNet P8*.

 [Configuring a Windows-based file server for a UNIX client](#)

For more information about the fsa1 directory, see *Plan and Prepare Your Environment for IBM FileNet P8*.

---

## Installing IBM FileNet Deployment Manager

IBM FileNet Deployment Manager works with Enterprise Manager to deploy test systems into full production. You can install the IBM FileNet Deployment Manager interactively or silently on a Windows machine.

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

FileNet Deployment Manager runs only on Windows.

To install IBM 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 Engine values, filter by **CE Installer** in the **Installation or Configuration Program** column.

2. On the machine where you will install FileNet Deployment 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 Windows components.

Option	Description
Microsoft Windows XP, Microsoft Windows Server 2003	Microsoft .NET Framework 2.0 and Web Services Enhancements (WSE) 3.0
Content Engine version 4.5.1 Fix Pack 002 or higher with Microsoft Windows Vista, Microsoft Windows Server 2008, or Microsoft Windows 7	Microsoft .NET Framework 3.0 and Windows Communication Foundation (WCF)

4. Access the Content Engine installation software.
5. Start the FileNet Deployment Manager installation.

Option	Description
Interactive installation	<ol style="list-style-type: none"> <li>1. Run the following command in the software package: P8CE-4.5.1-WIN.EXE</li> <li>2. Complete the program installation wizard by using the values from your worksheet.</li> </ol>
Silent installation	<ol style="list-style-type: none"> <li>1. Open the CE_silent_install.txt file in the software package for editing.</li> <li>2. Set the parameter values in the CE_silent_install.txt file for your site. Be sure to set the <b>CHOSEN_INSTALL_FEATURE_LIST</b> parameter value to <b>Tools</b> If you want to also install FileNet Enterprise Manager on this machine, select .NET Clients as well:<b>DotNetClients,Tools</b></li> <li>3. Set the LAUNCH_CM value to 0.</li> <li>4. Save your edits.</li> <li>5. Run the following command in the software package on a single line: P8CE-4.5.1-WIN.EXE -f CE_silent_install.txt -i silent</li> </ol>

To start FileNet Deployment Manager, choose **Start** → **All Programs** → **FileNet P8 Platform** → **P8 Deployment Manager**.

---

## 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 185

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 186

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"
```

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

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.

## Installing Workplace File Tracker

If you want to use the file tracking feature without installing Application Integration, you can install Workplace File Tracker. Complete the installation on each machine that will use Workplace File Tracker.

If you have already installed or upgraded to Application Integration 3.5.1-002 or higher, then the File Tracker feature has already been installed. Do not perform this procedure if you already installed a version of Application Integration that includes File Tracker, including Application Integration 4.0.

If you have already installed Application Integration 3.5.1-001 or earlier, upgrade it to 4.0 plus the latest fix pack, and this will include the File Tracker installation.

“Installing the File Tracker software interactively”

You can download File Tracker from Workplace. To run the File Tracker software installation, you must have Administrator privileges and use the General Author tools in Workplace.

“Installing the File Tracker software silently” on page 188

To install the File Tracker software silently, save the FileTracker.exe file locally and run it at the command line using the /s switch. You can include optional command line values when you run the installation program.

## Installing the File Tracker software interactively

You can download File Tracker from Workplace. To run the File Tracker software installation, you must have Administrator privileges and use the General Author tools in Workplace.

To install File Tracker interactively:

1. Log on 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 File Tracker** and 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 FileTracker.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 File Tracker 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 one of the following:
  - Click **Change** if you want to install File Tracker to a different location. Specify the location to which you want to install File Tracker, and then click **OK**. Click **Next**.
  - Click **Next** to accept the default location.
8. Click **Install**.
9. After the install is complete, click **Finish** to complete the setup process.
10. (On Vista using Internet Explorer 7.0 only) Add the Workplace URL to the browser security tab.
  - a. In the Internet Explorer 7.0 browser, click **Tools** → **Internet Options**. Click the **Security** tab.
  - b. Select Trusted Sites, and click the **Sites** button.
  - c. Add the Workplace URL and click **Add**.
  - d. Click **OK**, and **OK** again to save changes.

If you want file tracking to be available to all users who have downloaded the File Tracker application, set the Enable file tracking preference in the site

preferences. For more information, see **User Help** → **Actions, preferences, and tools** → **Site preferences** → **General preferences** → **File tracking**.

## Installing the File Tracker software silently

To install the File Tracker software silently, save the FileTracker.exe file locally and run it at the command line using the /s switch. You can include optional command line values when you run the installation program.

To install File Tracker software silently:

1. Log in to the client machine using an account that has Administrator privileges and sign in to Workplace.
2. Click **Author**, and then click **General Tools**.
3. Scroll down and click **Download File Tracker** and click **Save**. In the Save As dialog box, find a location on your machine in which to download and save the FileTracker.exe file locally, and then click **Save**.
4. Open a DOS command window and change the current directory to the one that contains FileTracker.exe.
5. Type the following at the command line:

```
FileTracker.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. In addition, be aware of spaces specified between switches in the above example. Using the correct spacing ensures a successful silent install.

Refer to the following optional command line values you can also use. Append the values within the string containing the msi arguments.

For example:

```
FileTracker.exe /s /v"/qn /L*v
C:\temp\FileTrackerSetup.txt LICENSE_ACCEPTED=true"
```

Command Line Values	Settings
/L*v C:\temp\FileTrackerSetup.txt	Verbose installation log and specific log location. If you intend to specify a log location, create the directory before running the silent install. If the directory is not created ahead of time, the install will fail.

6. (On Vista using Internet Explorer 7.0 only) Add the Workplace URL to the browser security tab as follows:
  - a. In the Internet Explorer 7.0 browser, click **Tools** → **Internet Options**. Click the **Security** tab.
  - b. Select Trusted Sites, and click the **Sites** button.
  - c. Add the Workplace URL and click **Add**.
  - d. Click **OK**, and **OK** again to save changes.

If you want file tracking to be available to all users who have downloaded the File Tracker application, set the Enable file tracking preference in the site preferences. For more information, see **User Help** → **Actions, preferences, and tools** → **Site preferences** → **General preferences** → **File tracking**.



---

## 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 190

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>
```

6. (For JBoss Application Server 5.0.1 only) Navigate to each custom copied Workplace jboss-classloading.xml instance and update the path for the name and domain. For example, in the *install\_path/FileNet/AE/Workplace1/WEB-INF/jboss-classloading.xml*, make the following changes to the name and domain values:

```
<classloading xmlns="urn:jboss:classloading:1.0"
 name="Workplace1.war"
 domain="Workplace1.war"
 export-all="NON_EMPTY"
 import-all="false">
</classloading>
```

## 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 (shown in **bold**, below).

```
<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, shown in bold:

```
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, shown in **bold**:

```
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 and/or interim fixes required. To determine whether such additional software updates are needed, contact your service representative.

---

## Enabling Application Engine to use ISRA

Image Services Resource Adaptor (ISRA) is a J2EE connector to the IBM FileNet Image Services libraries. Using ISRA, Workplace users can view 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 192 for details that might affect your collocation plans.
- Configure Workplace Site Preferences.

“ISRA SSL support” on page 192

The following table details supported SSL configurations for ISRA.

“Installing and deploying the Application Engine ISRA servlet” on page 192

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 194

Before using the ISRA servlet, you must enable the Image Services external service and set the ISRA Interface Servlet URL in Workplace Site Preferences.

“Logging in to Image Services by using an LDAP account” on page 194  
 In order to log in to Image Services by using your LDAP account, you must configure ISRA for LDAP authentication.

“Accessing Image Services library documents” on page 195  
 For information about accessing Image Services library documents, see **User Help** → **Actions, preferences and tools** → **Actions** → **Documents** → **Add a document (Workplace)**.

## ISRA SSL support

The following table details supported SSL configurations for ISRA.

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.

- Log on to the application server by using the following account, depending on your operating system:

Option	Description
UNIX	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.
Windows	A member of the local Administrators group or as a user account with equivalent permissions.

- Stop the application server if it is running.
- Access the ISRA installation package, and start the following Application Engine ISRA Servlet setup program, depending on your operating system:

Option	Description
UNIX	AE-ISRA-Servlet-4.0.2.0- <i>operating_system</i> .bin
Windows	AE-ISRA-Servlet-4.0.2.0-WIN.exe

- Complete the installation program screens by using the values from your worksheet.
- 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.
- 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.

- (WebSphere Application Server and WebLogic Server only) Start the application server.
- Deploy `AE_israservlet_install_path/FileNet/ApplicationEngineISRAServlet/ae_isra.war` in the same way you deployed the `app_engine.war` file for Workplace.
- (JBoss only) Start the application server.
- Verify the Application Engine ISRA Servlet is installed and deployed correctly, as follows. This step launches a diagnostic tool that does the verification.
  - Open your web browser.
  - 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
```

## Configuring Workplace site preferences for ISRA

Before using the ISRA servlet, you must enable the 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 Image Services by using an LDAP account

In order to log in to Image Services by using your LDAP account, you must configure ISRA for LDAP authentication.

To log in to the 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 Image Services, See the *Image Services System Tools Reference Manual*.

2. Configure Image Services for LDAP authentication.

If the LDAP account with which you accessed Workplace is not valid for the Image Services library, or if LDAP authentication is not configured, you will be prompted to log in to the Image Services library.

## Accessing Image Services library documents

For information about accessing Image Services library documents, see **User Help** → **Actions, preferences and tools** → **Actions** → **Documents** → **Add a document** (Workplace).

---

## Installing and configuring IBM System Dashboard for Enterprise Content Management

Content Engine, Application Engine, and Process Engine install, by default, the necessary software required for the System Manager performance component. To use System Manager, enable associated components and install IBM System Dashboard for Enterprise Content Management to perform related configuration procedures to enable System Manager.

Installing Dashboard is not necessary if you currently have IBM FileNet System Monitor installed.

See the following IBM FileNet P8 help topic **FileNet P8 Documentation** → **System Administration** → **Enterprise-wide Administration** → **System Manager** for instructions on how to enable the associated System Manager components.

See the documentation provided with IBM System Dashboard for Enterprise Content Management for instructions on how to use Dashboard.

---

## Modifying an Autonomy K2 server configuration

You can add Autonomy K2 servers or move existing servers to new hardware.

“Adding additional K2 administration servers”

You must install additional Autonomy K2 Administration Servers to handle the indexing load. The Master Administration Server is the main hub for configuring all the servers you install. The additional servers are managed through the K2 Dashboard that is installed with the Master Administration Server.

“Moving Autonomy K2 servers to new hardware” on page 202

To move an existing installation of the Autonomy K2 Master Administration server configuration, the installation must be imaged and then restored on the new hardware. If any details of the new configuration do not match the previous configuration, the configuration will not work.

## Adding additional K2 administration servers

You must install additional Autonomy K2 Administration Servers to handle the indexing load. The Master Administration Server is the main hub for configuring



all the servers you install. The additional servers are managed through the K2 Dashboard that is installed with the Master Administration Server.

**Important:** A K2 Master Administration Server must be installed before you add additional K2 Administration Servers.

“Installing additional Autonomy K2 administration servers (UNIX)”

You can install additional Autonomy K2 servers as part of a Content Search Engine configuration.

“Starting or stopping the Autonomy K2 services (UNIX)” on page 199

You can start or stop the Autonomy K2 services using manual commands, according to your environment.

“Installing additional Autonomy K2 administration servers (Windows)” on page 200

You can install additional Autonomy K2 servers as part of a Content Search Engine configuration.

“Configuring additional K2 administration servers” on page 201

If you want to add and use additional K2 Index Servers or Search Servers in an existing configuration, you must enable them through Enterprise Manager.

### Installing additional Autonomy K2 administration servers (UNIX)

You can install additional Autonomy K2 servers as part of a Content Search Engine configuration.

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

To install interactively, X-Terminal must be installed on the UNIX server.

**Important:** Most processes for the Autonomy K2 software will run as *k2\_os\_user*. However, the *vspget* process must run as root. For details on required accounts and related permissions, see *Plan and Prepare Your Environment for IBM FileNet P8*.

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 Search Engine values, filter by **CSE Installer** in the **Installation or Configuration Program** column.

2. Access the host machine and log on as a user with root privileges.
3. Enter the following commands to set the *setuid* bit of the *vspget* program so that the service runs as root:

```
chown root verity_install_path/k2/_platform/bin/vspget
```

```
chmod u+s verity_install_path/k2/_platform/bin/vspget
```

Replace *\_platform* with the following directory.

Table 16. Directory by platform

Platform	Directory
HPUX	<i>_hpux</i>
AIX	<i>_rs6k43</i>
Solaris	<i>_ssol26</i>
Linux	<i>_ilnx21</i>

4. Log off the machine.

5. Log on to the machine as *k2\_os\_user*.
6. Set the following environment variable and place the entry in the *.profile* file for *k2\_os\_user*.
 

```
JAVA_HOME=java_(JDK)_install_path/jdkversion
export JAVA_HOME
```
7. Access the IBM FileNet P8 Content Search Engine installation package.
8. In the *.profile* file for *k2\_os\_user*, set the *PATH*, *SHLIB\_PATH*, *LIBPATH*, and *LD\_LIBRARY\_PATH* environment variables (depending on your operating system), each on its own line, without line breaks.

**Important:** If your *.profile* file has a line containing `set -u` that appears before the lines involving *PATH*, *SHLIB\_PATH*, *LIBPATH*, or *LD\_LIBRARY\_PATH*, you must do one of the following edits before setting the environment variables:

- Remove the line containing `set -u` from the *.profile* file.
- Move the line containing `set -u` to a point in the *.profile* file below the lines involving *PATH*, *SHLIB\_PATH*, *LIBPATH*, or *LD\_LIBRARY\_PATH*.

#### AIX

```
PATH=$PATH:verity_install_path/k2/_rs6k43/bin
export PATH
LIBPATH=$LIBPATH:verity_install_path/k2/_rs6k43/bin
export LIBPATH
```

#### HP-UX

```
PATH=$PATH:verity_install_path/k2/_hpux/bin
export PATH
SHLIB_PATH=$SHLIB_PATH:verity_install_path/k2/_hpux/bin
export SHLIB_PATH
```

#### Linux

```
PATH=$PATH:verity_install_path/k2/_ilnx21/bin
export PATH
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:verity_install_path/k2/_ilnx21/bin
export LD_LIBRARY_PATH
```

#### Solaris

```
PATH=$PATH:verity_install_path/k2/_sso126/bin
export PATH
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:verity_install_path/k2/_sso126/bin
export LD_LIBRARY_PATH
```

9. Start the installation interactively or silently:
  - “Installing additional Autonomy K2 administration servers interactively (UNIX)”
  - To install Content Search Engine interactively, you run a program wizard.
  - “Installing additional Autonomy K2 administration servers silently (UNIX)” on page 198
  - When you install Content Search Engine silently, you run a command in the Content Search Engine software package that references parameters in an installation text file.
  - “Setting environment variables for Content Search Engine (UNIX)” on page 198
  - Content Search Engine requires environment variables to be added to the *.profile* file of the Autonomy K2 operating system user.

#### **Installing additional Autonomy K2 administration servers interactively (UNIX):**

To install Content Search Engine interactively, you run a program wizard.

To install additional Autonomy K2 administration servers interactively:

1. Run one of the following commands:

Platform	Command
HPUX	P8CSE-4.5.1.0-HPUX.BIN
AIX	P8CSE-4.5.1.0-AIX.BIN
Solaris	P8CSE-4.5.1.0-SOL.BIN
Linux	P8CSE-4.5.1.0-LINUX.BIN

2. Complete the installation screens using the values in your worksheet.
3. Review the following Content Search Engine log files for installation errors. The files are located in the verity directory of the installation path:
  - `cse_install_path/verity/cse_install_log_4_5_1.txt`
  - `cse_install_path/verity/vconfig.log`

### Installing additional Autonomy K2 administration servers silently (UNIX):

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

To install Content Search Engine silently:

1. Edit the `CSE_silent_install.txt` file to reflect the appropriate responses for your installation using the values in your worksheet.
2. Run the following command: Run the following command.

*Table 17. Silent installation commands by platform*

Platform	Command
HPUX	P8CSE-4.5.1.0-HPUX.BIN -f CSE_silent_install.txt -i silent
AIX	P8CSE-4.5.1.0-AIX.BIN -f CSE silent install.txt -i silent
Linux	P8CSE-4.5.1.0-LINUX.BIN -f CSE_silent_install.txt -i silent
Solaris	P8CSE-4.5.1.0-SOL.BIN -f CSE_silent_install.txt -i silent

3. Review the following Content Search Engine log files for installation errors. The files are located in the verity directory of the installation path:
  - `cse_install_path/verity/cse_install_log_4_5_1.txt`
  - `cse_install_path/verity/vconfig.log`

### Setting environment variables for Content Search Engine (UNIX):

Content Search Engine requires environment variables to be added to the `.profile` file of the Autonomy K2 operating system user.

To set environment variables:

In the `.profile` file for `k2_os_user`, set the `PATH`, `SHLIB_PATH`, `LIBPATH`, and `LD_LIBRARY_PATH` environment variables (depending on your operating system), each on its own line, without line breaks.

**Important:** If your `.profile` file has a line containing `set -u` that appears before the lines involving `PATH`, `SHLIB_PATH`, `LIBPATH`, or `LD_LIBRARY_PATH`, you must do one of the following edits before setting the environment variables:

- Remove the line containing `set -u` from the `.profile` file.
- Move the line containing `set -u` to a point in the `.profile` file below the lines involving `PATH`, `SHLIB_PATH`, `LIBPATH`, or `LD_LIBRARY_PATH`.

#### AIX

```
PATH=$PATH:verity_install_path/k2/_rs6k43/bin
export PATH
LIBPATH=$LIBPATH:verity_install_path/k2/_rs6k43/bin
export LIBPATH
```

#### HP-UX

```
PATH=$PATH:verity_install_path/k2/_hpux/bin
export PATH
SHLIB_PATH=$SHLIB_PATH:verity_install_path/k2/_hpux/bin
export SHLIB_PATH
```

#### Linux

```
PATH=$PATH:verity_install_path/k2/_ilnx21/bin
export PATH
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:verity_install_path/k2/_ilnx21/bin
export LD_LIBRARY_PATH
```

#### Solaris

```
PATH=$PATH:verity_install_path/k2/_sso126/bin
export PATH
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:verity_install_path/k2/_sso126/bin
export LD_LIBRARY_PATH
```

### Starting or stopping the Autonomy K2 services (UNIX)

You can start or stop the Autonomy K2 services using manual commands, according to your environment.

To manually start or stop the Autonomy K2 services on which Content Search Engine relies, you must use the commands provided by Autonomy. (Each command is to be typed on one line.)

Option	Description
AIX	Start services: <pre>nohup verity_install_path /k2/_rs6k43/bin/k2adminstart &amp;</pre> Stop services: <pre>verity_install_path /k2/_rs6k43/bin/k2adminstop</pre>
HP-UX	Start services: <pre>nohup verity_install_path /k2/_hpux/bin/k2adminstart &amp;</pre> Stop services: <pre>verity_install_path /k2/_hpux/bin/k2adminstop</pre>

Option	Description
Solaris	Start services: <pre>nohup verity_install_path /k2/_sso126/bin/k2adminstart &amp;</pre> Stop services: <pre>verity_install_path /k2/_sso126/bin/k2adminstop</pre>
Linux	Start services: <pre>nohup verity_install_path /k2/_i1nx21/bin/k2adminstart &amp;</pre> Stop services: <pre>verity_install_path /k2/_i1nx21/bin/k2adminstop</pre>

### Installing additional Autonomy K2 administration servers (Windows)

You can install additional Autonomy K2 servers as part of a Content Search Engine configuration.

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

To install Content Search 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 Search Engine values, filter by **CSE Installer** in the **Installation or Configuration Program** column.

2. Log on to the host machine as *k2\_os\_user*.
3. Install Content Search Engine interactively or silently:
  - “Installing additional Autonomy K2 administration servers interactively (Windows)”  
To install Content Search Engine interactively, you run a program wizard.
  - “Installing additional Autonomy K2 administration servers silently (Windows)”  
on page 201  
When you install Content Search Engine silently, you run a command in the Content Search Engine software package that references parameters in an installation text file.

### Installing additional Autonomy K2 administration servers interactively (Windows):

To install Content Search Engine interactively, you run a program wizard.

To install Content Search Engine interactively:

1. Access the IBM FileNet P8 Content Search Engine installation package and run the P8CSE-4.5.1WIN.EXE file.
2. Complete the installation program screens by using the values in your worksheet.
3. Review the following Content Search Engine log files for installation errors. The files are located in the *verity* directory of the installation path:

- *verity\_install\_path*\cse\_install\_log\_4\_5\_1.txt
- *verity\_install\_path*\vconfig.log

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

4. Verify that the following two Windows services are installed on your machine after the installation finishes:
  - Verity K2 6.2.1 Administration Server service
  - Verity K2 Administration Web Server service (Tomcat server)

### Installing additional Autonomy K2 administration servers silently (Windows):

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

To install Content Search Engine silently:

1. Edit the *cse\_silent\_install.txt* file to reflect the appropriate responses for your installation by using the values from your worksheet.
2. Run the IBM FileNet P8 Content Search Engine installation program by executing the following command:
 

```
P8CSE-4.5.1-WIN.EXE -f CSE_silent_install.txt -i silent
```
3. Review the following Content Search Engine log files for installation errors. The files are located in the *verity* directory of the installation path:
  - *verity\_install\_path*\cse\_install\_log\_4\_5\_1.txt
  - *verity\_install\_path*\vconfig.log

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

4. Verify that the following two Windows services are installed on your machine after the installation finishes:
  - Verity K2 6.2.1 Administration Server service
  - Verity K2 Administration Web Server service (Tomcat server)

### Configuring additional K2 administration servers

If you want to add and use additional K2 Index Servers or Search Servers in an existing configuration, you must enable them through Enterprise Manager.

1. Log on to Enterprise Manager as the GCD Administrator and expand the Enterprise Manager tree.
2. Open the Index Area folder.
3. Right-click the index area that you want to add the new services to and select **Properties**.
4. Enable the new Search Servers as follows:
  - a. Click **Edit Search Servers**.
  - b. In the Search Servers Available pane, highlight any servers you want to enable for this index area and click **Add** to add the server to the Search Servers Selected list.

- c. Click **OK** to save the settings and enable the new servers.
5. Enable the new Index Servers as follows:
  - a. Click **Edit Index Servers**.
  - b. In the Index Servers Available pane, highlight any servers you want to enable for this index area and click **Add** to add the server to the Index Servers Selected list.
  - c. Click **OK** to save the settings and enable the new servers.

## Moving Autonomy K2 servers to new hardware

To move an existing installation of the Autonomy K2 Master Administration server configuration, the installation must be imaged and then restored on the new hardware. If any details of the new configuration do not match the previous configuration, the configuration will not work.

To move K2 Master Administration Server software to new hardware:

1. Back up your Autonomy K2 Master Administration Server configuration.
2. Configure the new machine.
3. Restore your Autonomy K2 Master Administration Server installation.

“Moving K2 administration server software to new hardware”

Follow this procedure to maintain your existing configuration on new hardware. Alternatively, you can remove the server from your configuration (see procedure below) and then create a new configuration after installing the K2 Administration Server software.

“Removing K2 administration servers from your Content Search Engine configuration” on page 203

To remove K2 administration servers from your Content Search Engine configuration, remove the appropriate K2 Administration server from the dashboard configuration.

## Moving K2 administration server software to new hardware

Follow this procedure to maintain your existing configuration on new hardware. Alternatively, you can remove the server from your configuration (see procedure below) and then create a new configuration after installing the K2 Administration Server software.

To move your existing configuration to new hardware, your new hardware must be configured the same as the previous machine. All drives and shares must be named the same and each server must have the same host name and IP addresses.

1. Take careful note of all aspects of your current Content Search Engine configuration. Record all share names, host names, server ports, and IP addresses. Record the server names and ports of all configured server services in the K2 Dashboard, and their locations.
2. If collections are stored on this machine, make a backup copy.
3. Set up your new hardware and ensure the machine host name and IP address match your previous configuration.
4. Follow the Add Additional K2 Administration Servers procedure above to install the K2 Administration Server software on the new machine.
5. Create the services for this machine in the K2 Master Administration Server dashboard and ensure all server services are named the same as your previous configuration and ensure all servers created in the Autonomy K2 Dashboard are named the same and configured for the same ports.



You can change the ports; but if you do so, must reboot the Content Engine servers. The names of the search servers, index servers and brokers might not be changed for any items referenced by an index area on the CE.

6. Restore the collections to the same Root Dir Path (as specified in the index area properties) as before. If the collections are no longer available, mark those collections as unavailable, and then run a reindexing job on those collections. Otherwise copy/restore those collections via whatever tool you used to save them.
7. Modify the appropriate directory path entries in the `Verity.cfg` file.

## Removing K2 administration servers from your Content Search Engine configuration

To remove K2 administration servers from your Content Search Engine configuration, remove the appropriate K2 Administration server from the dashboard configuration.

1. If collections were stored on the machine you want to remove:
  - a. Determine which K2 Server will hold the collections. On that machine, create a new collections directory and temp directory and assign the appropriate permissions. For details, see “Creating a Content Search Engine collections directory” on page 96.  
  
**Important:** See the index area properties (Root Dir Path) for the collections location for the appropriate index area.
  - b. Modify the appropriate directory path entries in the `verity.cfg` file.
  - c. Move the collections to the new location.
2. Modify the index area to use the index servers and search servers of the machine to which the collections were moved.
3. Access the K2 Dashboard and remove the appropriate K2 Administration server from the dashboard configuration.

---

## Installing the COM compatibility layer (CCL)

The option to install the COM compatibility layer is available as part of the IBM FileNet P8 Content Engine installer.

To install the COM Compatibility Layer (CCL) from the IBM FileNet Content Engine installer:

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 installing later by running the Content Engine installer again. You can also install the CCL anytime by using the Configuration Manager tool.



---

## Part 2. Upgrading and configuring IBM FileNet P8 Platform

Upgrading the IBM FileNet P8 Platform software can require that you make installation and configuration changes to one or more of the core application components and the common documentation, and the upgrade process can vary depending on the product version you are currently running.

**Important:** You must upgrade the core components before you upgrade any expansion products or optional add-on components.

“Upgrading IBM FileNet P8 documentation” on page 207

You can point your IBM FileNet P8 components to the information center on [ibm.com](http://ibm.com). You can also choose to upgrade your existing IBM FileNet P8 documentation server by installing the new files and redeploying the documentation on the Web application server.

“Upgrading and configuring Content Engine and Content Search Engine” on page 217

You can upgrade Content Engine and Content Search Engine to version 4.5.1 from version 3.5.2, 4.0.1, or 4.5.0.

“Upgrading and configuring Process Engine” on page 391

Upgrade the Process Engine by performing several pre-upgrade steps, installing the Process Engine software and performing multiple post-upgrade steps.

“Upgrading and configuring Application Engine” on page 439

You can upgrade Application Engine from version 3.5 or version 4.0 to version 4.0.2. The procedures for upgrading Application Engine vary depending on the version that you are upgrading.

“Upgrading add-on components” on page 487

You must upgrade all of the IBM FileNet P8 Platform core components before upgrading the add-on components listed in this topic.



---

## Upgrading IBM FileNet P8 documentation

You can point your IBM FileNet P8 components to the information center on [ibm.com](http://ibm.com). You can also choose to upgrade your existing IBM FileNet P8 documentation server by installing the new files and redeploying the documentation on the Web application server.

You can link your FileNet P8 software directly to the IBM FileNet P8 Platform Version 4.5.1 information center on [www.ibm.com](http://www.ibm.com). The advantages of linking to the [ibm.com](http://ibm.com) information center are as follows:

- You do not have to maintain a documentation server or information center.
- The documentation is always up to date.

If you want to use the online information center, you do not need to install or upgrade any documentation in your environment. However, you must configure your IBM FileNet P8 Platform components to use the new P8 documentation URL:

<http://publib.boulder.ibm.com/infocenter/p8docs/v4r5m1/topic/com.ibm.p8.doc>

To change the documentation URL for your FileNet P8 components, see the following help topics:

- **IBM FileNet P8 documentation** → **System Administration** → **Content Engine Administration** → **FileNet P8 domain** → **How to...** → **Configuring the FileNet P8 Platform documentation location**
- **IBM FileNet P8 documentation** → **System Administration** → **Process Administration** → **System administration tasks** → **Configure optional features** → **Reconfigure the FileNet documentation server URL**

You can also choose to upgrade your existing documentation package installation. You must also rebuild the documentation search index if you upgrade an installation containing more than the core IBM FileNet P8 Platform documentation.

Consider the following details as you get ready to upgrade your documentation:

- As of the IBM FileNet P8 4.0 release, you can deploy the IBM FileNet P8 documentation on a Content Engine server. Like Application Engine, Content Engine 4.0 and later runs on a web application server. If you are an existing 3.5 customer and want to install the 4.5.1 documentation onto a Content Engine server or a new application server, you must do a new installation rather than an upgrade.
- Before you update any IBM FileNet P8 documentation, review the *IBM FileNet P8 Hardware and Software Requirements* for the required software versions and updates for vendor software.
- Although some versions of Oracle WebLogic Server support deployment of web applications based on WAR files, you cannot deploy `ecm_help.war` on this application server platform. Instead you must use the fully expanded IBM FileNet P8 documentation `ecm_help` directory structure. Otherwise, the searches within the IBM FileNet P8 documentation do not work and you receive null pointer errors.
- In environments where Microsoft Windows NTFS is used, there is a 256 character limit on file and directory names (directory depth). When trying to delete an existing IBM FileNet P8 documentation Web site, you might encounter

access denied errors. See Microsoft Knowledge Base article <http://support.microsoft.com/?kbid=320081> for more information.

- Before you install the latest IBM FileNet P8 documentation, be sure to back up your existing IBM FileNet P8 documentation Web site according to your site and application server procedures. This precaution allows you to restore the IBM FileNet P8 documentation Web site quickly if for any reason you have to back out of or delay your IBM FileNet P8 software upgrade.
- If you install any IBM FileNet P8 expansion products as part of your upgrade, be aware of the following requirements:
  - You must copy the associated documentation for all expansion products onto the updated IBM FileNet P8 documentation server.
  - You must update the index for the documentation Search feature as documented. This action ensures that searches return all expected results. If you add documentation for other expansion products later, you must rerun the procedure for updating the documentation Search index.
  - You must also update the documentation Search index if you update the installed IBM FileNet P8 documentation that you have customized or translated as part of your own application development.
- Any time you update the documentation search index, a backup of the files in the existing Index/core directory is automatically copied to the Index/Index01d subdirectory. If you need to return to your previous indexed state, you can reapply these backed-up files to the core subdirectory. However, you must first remove any newer existing files at that location.
- Depending on your operating system and application server levels, your options might vary slightly from what is documented.

To upgrade the documentation requires that you copy new files to the documentation server and reindex those files as necessary. You can then redeploy, start, and verify the upgraded documentation web application.

“Refreshing or updating IBM FileNet P8 documentation” on page 209

You can choose one of two methods to upgrade an IBM FileNet P8 documentation installation. The method you choose depends on whether the existing installation includes expansion product and other documentation in addition to core IBM FileNet P8 Platform documentation.

“Updating the documentation search index” on page 213

You must update the documentation search index only if you add to the core IBM FileNet P8 Platform documentation that is installed on an application server. For example, you must perform this task if you add expansion product documentation or auxiliary documentation such as release notes or technical notices. You must also update the search index any time you install an update of one of these collocated pieces of documentation.

“Starting and verifying the IBM FileNet P8 documentation web application” on page 214

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

---

## Refreshing or updating IBM FileNet P8 documentation

You can choose one of two methods to upgrade an IBM FileNet P8 documentation installation. The method you choose depends on whether the existing installation includes expansion product and other documentation in addition to core IBM FileNet P8 Platform documentation.

“Refreshing IBM FileNet P8 documentation without uninstalling”

You can refresh an existing IBM FileNet P8 documentation installation by copying the newer documentation directly over the existing files. Use this method if you have only the core IBM FileNet P8 Platform documentation installed and it is version 3.5 or later.

“Updating IBM FileNet P8 documentation by uninstalling and reinstalling” on page 210

If your existing documentation installation includes both core IBM FileNet P8 Platform documentation and other IBM FileNet P8 documentation, you must uninstall it completely before you can upgrade it.

### Refreshing IBM FileNet P8 documentation without uninstalling

You can refresh an existing IBM FileNet P8 documentation installation by copying the newer documentation directly over the existing files. Use this method if you have only the core IBM FileNet P8 Platform documentation installed and it is version 3.5 or later.

If you update the core documentation package, you must also reindex the files for search support as a follow-up task.

**Important:**

- If you have IBM FileNet P8 3.5 or later documentation installed with expansion product documentation included, use the procedure “Updating IBM FileNet P8 documentation by uninstalling and reinstalling” on page 210.
- This refresh procedure requires that you copy the expanded `ecm_help` directory from the IBM FileNet P8 Documentation package over the existing documentation. This stipulation applies to all application server types, even those types such as IBM WebSphere Application Server that required a WAR file for initial deployment.

To refresh the IBM FileNet P8 documentation without first uninstalling it:

1. Stop the IBM FileNet P8 documentation Web application or the application server on which the existing documentation is deployed so that no processes can access the documentation.
2. On the IBM FileNet P8 documentation application server, locate the deployed IBM FileNet P8 documentation directory and back up the search-index files located in:

Option	Description
UNIX	<code>deployment_path/ecm_help/search/index/core</code>
Windows	<code>deployment_path\ecm_help\search\index\core</code>

3. Access the new IBM FileNet P8 Platform documentation package.
4. Copy the expanded `ecm_help` directory from the package over the deployed `ecm_help` directory.



5. As a best practice, download the latest web-posted updates of the planning and installation guides. For IBM FileNet P8 Platform, copy these PDF files to the `ecm_help/installation` directory on your IBM FileNet P8 documentation server.
6. (Optional) Download any auxiliary documentation to the `ecm_help/installation/web` directory on your IBM FileNet P8 Platform documentation server.
7. Continue with one of the following tasks:
  - If you added documentation to the core IBM FileNet P8 Platform documentation, then continue with “Updating the documentation search index” on page 213.
  - If you added no other documentation to the core IBM FileNet P8 Platform documentation, then continue with “Starting and verifying the IBM FileNet P8 documentation web application” on page 214.

#### Related information

 Product documentation for IBM FileNet P8 Platform  
Download updated PDF's of the IBM FileNet P8 Platform documentation.

## Updating IBM FileNet P8 documentation by uninstalling and reinstalling

If your existing documentation installation includes both core IBM FileNet P8 Platform documentation and other IBM FileNet P8 documentation, you must uninstall it completely before you can upgrade it.

Use the procedure provided for your application server type.

“Updating the IBM FileNet P8 documentation on IBM WebSphere Application Server”

To update IBM FileNet P8 documentation running on IBM WebSphere Application Server, you must uninstall the existing web application and then install the new documentation files.

“Updating the IBM FileNet P8 documentation on Oracle WebLogic Server” on page 211

To update IBM FileNet P8 documentation running on Oracle WebLogic Server, you must stop the existing web application and then install the new documentation files.

“Updating the IBM FileNet P8 documentation on JBoss Application Server” on page 212

To update IBM FileNet P8 documentation running on JBoss Application Server, you must stop the existing web application and then install the new documentation files.

### Updating the IBM FileNet P8 documentation on IBM WebSphere Application Server

To update IBM FileNet P8 documentation running on IBM WebSphere Application Server, you must uninstall the existing web application and then install the new documentation files.

To update the documentation:

1. Verify that the IBM WebSphere Application Server machine is running, and then start the WebSphere administrative console.
2. From the WebSphere administrative console, choose **Uninstall** to remove the existing documentation site.

3. From the initial installation location, delete the installed IBM FileNet P8 documentation files but leave the `ecm_help` directory in place.
4. Copy the IBM FileNet P8 `ecm_help.war` file from the IBM FileNet P8 documentation package to the local hard disk drive.
5. From the WebSphere administrative console, deploy the `ecm_help.war` file by using `ecm_help` as the Context Root.
6. For each expansion product, copy the expanded `ecm_help` directory from the package over the deployed `ecm_help` directory.  
You can copy more than one expansion product documentation set to the documentation server before continuing, for example, for Content Federation Services and IBM InfoSphere Enterprise Records. When you are finished, you have one `ecm_help` directory structure containing files for the core documentation and one or more sets of expansion product documentation.
7. As a best practice, download the latest Web-posted updates of the planning and installation guides. For IBM FileNet P8 Platform, copy these PDF files to the `ecm_help/installation` directory on your IBM FileNet P8 documentation server. Check the documentation page on the IBM customer support Web site <http://www.ibm.com/software/data/support/> for the latest versions of these guides.
8. (Optional) Download any auxiliary documentation to the `ecm_help/installation/web` directory on your IBM FileNet P8 Platform documentation server.
9. From the WebSphere administrative console, restart the IBM FileNet P8 documentation site.
10. Continue with one of the following tasks:
  - If you added expansion products, continue with “Updating the documentation search index” on page 213.
  - If you have no further documentation to install, continue with “Starting and verifying the IBM FileNet P8 documentation web application” on page 214.

### **Updating the IBM FileNet P8 documentation on Oracle WebLogic Server**

To update IBM FileNet P8 documentation running on Oracle WebLogic Server, you must stop the existing web application and then install the new documentation files.

To update the documentation:

1. Verify that the Oracle WebLogic Server machine is running, and then start the WebLogic Administration Console.
2. From the WebLogic Administration Console, stop the existing documentation site.
3. From the initial installation location, delete the installed IBM FileNet P8 documentation files but leave the `ecm_help` directory in place.
4. Copy the `ecm_help` directory structure from the IBM FileNet P8 documentation package to the location of the original IBM FileNet P8 documentation.
5. For each expansion product, copy the expanded `ecm_help` directory from the package over the deployed `ecm_help` directory.

You can copy more than one expansion product documentation set to the documentation server before continuing, for example, for Content Federation Services and IBM InfoSphere Enterprise Records. When you are finished, you

have one `ecm_help` directory structure containing files for the core documentation and one or more sets of expansion product documentation.

6. As a best practice, download the latest Web-posted updates of the planning and installation guides. For IBM FileNet P8 Platform, copy these PDF files to the `ecm_help/installation` directory on your IBM FileNet P8 documentation server. Check the documentation page on the IBM customer support Web site <http://www.ibm.com/software/data/support/> for the latest versions of these guides.
7. (Optional) Download any auxiliary documentation to the `ecm_help/installation/web` directory on your IBM FileNet P8 Platform documentation server.
8. From the WebLogic Administration Console, restart the IBM FileNet P8 documentation site.
9. Continue with one of the following tasks:
  - If you added expansion products, continue with “Updating the documentation search index” on page 213.
  - If you have no further documentation to install, continue with “Starting and verifying the IBM FileNet P8 documentation web application” on page 214.

### **Updating the IBM FileNet P8 documentation on JBoss Application Server**

To update IBM FileNet P8 documentation running on JBoss Application Server, you must stop the existing web application and then install the new documentation files.

1. Shut down the Oracle WebLogic Server machine.
2. From the initial installation location, delete the IBM FileNet P8 documentation files but leave the `ecm_help` directory in place.
3. Delete the temporary working directory for the IBM FileNet P8 documentation from the `JBoss_home/work/MainEngine/localhost` directory.
4. Copy the `ecm_help` directory structure from the IBM FileNet P8 documentation package to the location of the original IBM FileNet P8 documentation.
5. For each expansion product, copy the expanded `ecm_help` directory from the package over the deployed `ecm_help` directory.

You can copy more than one expansion product documentation set to the documentation server before continuing, for example, for Content Federation Services and IBM InfoSphere Enterprise Records. When you are finished, you have one `ecm_help` directory structure containing files for the core documentation and one or more sets of expansion product documentation.
6. As a best practice, download the latest Web-posted updates of the planning and installation guides. For IBM FileNet P8 Platform, copy these PDF files to the `ecm_help/installation` directory on your IBM FileNet P8 documentation server. Check the documentation page on the IBM customer support Web site <http://www.ibm.com/software/data/support/> for the latest versions of these guides.
7. (Optional) Download any auxiliary documentation to the `ecm_help/installation/web` directory on your IBM FileNet P8 Platform documentation server.
8. Continue with one of the following tasks:
  - If you have added expansion products, then on to the procedure in “Updating the documentation search index” on page 213.

- If you have no further documentation to install, then go on to the procedure in “Starting and verifying the IBM FileNet P8 documentation web application” on page 214.

---

## Updating the documentation search index

You must update the documentation search index only if you add to the core IBM FileNet P8 Platform documentation that is installed on an application server. For example, you must perform this task if you add expansion product documentation or auxiliary documentation such as release notes or technical notices. You must also update the search index any time you install an update of one of these collocated pieces of documentation.

If no conditions require you to update the search index, skip to “Starting and verifying the IBM FileNet P8 documentation web application” on page 214.

To update the help Search index:

1. If the IBM FileNet P8 documentation Web application (ecm\_help) is running, stop it. Verify that no processes are accessing this documentation Web application.

**Important:** Ensure that you copied all the IBM FileNet P8 Platform expansion-products and auxiliary documentation that you intend to use to the application server location containing the core IBM FileNet P8 Platform documentation. Otherwise, you must repeat this procedure if you install additional documentation later.

2. Open a terminal or command prompt on the application server.
3. From the command line, navigate to the search subdirectory under the application root directory, for example, ecm\_help.
4. Complete the search indexing steps:

Option	Description
UNIX	<ol style="list-style-type: none"> <li>1. If not already done, apply <code>chmod 755</code> permissions on the <code>indexFiles.sh</code> file, which is preset to read-only permissions in the documentation package.</li> <li>2. Using a text editor, open the <code>indexFiles.sh</code> file.</li> <li>3. If necessary for your environment, set the <code>JAVA_HOME</code> variable in the script file with the path to your Java Runtime Environment (JRE) installation location. <b>Important:</b> The Java JRE installation subdirectory can be user-defined, so substitute your actual location.</li> <li>4. Save your changes and close the text editor.</li> <li>5. From the <code>ecm_help/search</code> directory, run the updated <code>indexFiles.sh</code> search-indexing script file.  As you run the script file, you might notice periodic Parse Abort errors. You can ignore these error conditions because they are benign and do not affect the overall indexing process.</li> </ol>

Option	Description
Windows	<ol style="list-style-type: none"> <li>1. If not already done, modify the search-indexing script file by setting Read and Execute permissions on the indexFiles.bat file, which is preset to read-only permissions in the documentation package.</li> <li>2. Using a text editor, open the indexFiles.bat search-indexing script file.</li> <li>3. If necessary for your environment, set the JAVA_HOME variable in the script file with the path to your Java Runtime Environment (JRE) installation location. <b>Important:</b> The Java JRE installation subdirectory can be user-defined, so substitute your actual location.</li> <li>4. Save your changes and close the text editor.</li> <li>5. From the ecm_help/search directory, run the updated indexFiles.bat search-indexing script file.  As you run the script file, you might notice periodic Parse Abort errors. You can ignore these error conditions because they are benign and do not affect the overall indexing process.</li> </ol>

## Starting and verifying the IBM FileNet P8 documentation web application

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

To verify the IBM FileNet P8 documentation installation:

1. Start the IBM FileNet P8 documentation Web application (ecm\_help) on the application server.
2. 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/ecm_help/
Oracle WebLogic Server	http://yourdocserver:7001/ecm_help/
JBoss Application Server	http://yourdocserver:8080/ecm_help/

If the installation was a success, the IBM FileNet P8 documentation opens the same way as for an IBM FileNet P8 component application.

3. Note the URL for your application server because you must enter it as the documentation URL for the IBM FileNet P8 components while running installation programs or setting site preferences later, for example, in Workplace or Workplace XT.

4. Click the **Search** link on the Help Directory toolbar and verify that it opens the documentation Search page.
5. Enter a value for your Search query and verify that the query runs as expected.
6. Select one of the Search query result links and verify that the help page opens.





---

# Upgrading and configuring Content Engine and Content Search Engine

You can upgrade Content Engine and Content Search Engine to version 4.5.1 from version 3.5.2, 4.0.1, or 4.5.0.

**Important:** In some customized versions of this documentation, Content Search Engine information is removed from this topic and its subtopics.

Perform the following upgrade tasks that apply to your existing version of Content Engine and Content Search Engine.

“Upgrading from version 3.5.2”

Upgrading Content Engine and Content Search Engine from version 3.5.2 is a multi-step process.

“Upgrading from version 4.0.1 or 4.5.0” on page 332

Upgrading Content Engine and Content Search Engine from version 4.0.1 or 4.5.0 is a multi-step process.

---

## Upgrading from version 3.5.2

Upgrading Content Engine and Content Search Engine from version 3.5.2 is a multi-step process.

**Important:** Before you start to upgrade the Content Engine software, ensure that you are at the correct version and fix pack level, as indicated in *Plan and Prepare Your Environment for IBM FileNet P8*.

1. “Completing pre-upgrade Content Engine configuration” on page 218  
You must complete several pre-upgrade procedures to prepare the Content Engine for an upgrade from version 3.5.2.
2. “Upgrading Content Engine and related client software” on page 224  
If you are upgrading from Content Engine version 3.5.2 on Windows, you can upgrade and continue to use Windows, or you can migrate your Content Engine to UNIX.
3. “Configuring Content Engine” on page 233  
You can configure and deploy all of your Content Engine instances by using Configuration Manager. A single Content Engine application instance equates to one deployed application on your application server.
4. “Deploying upgraded Content Engine instances” on page 259  
You must deploy the upgraded Content Engine on the web application server. Deploying makes the Content Engine application available for use.
5. “Installing storage device source files” on page 262  
If your upgraded IBM FileNet P8 system includes Tivoli Storage Manager or EMC Centera devices, you must install files on the Content Engine server.
6. “Completing Content Engine post-deployment steps” on page 272  
You must complete several Content Engine post-deployment steps before you can put an IBM FileNet P8 system into production.
7. “Installing the latest Content Engine client files on other IBM FileNet P8 servers (for staged upgrades)” on page 276  
When you upgrade Content Engine software, you must also upgrade the

associated Content Engine Client files installed on other machines running IBM FileNet P8 components, for example, on Process Engine and Application Engine servers.

8. “Establishing the FileNet P8 domain and Global Configuration Data” on page 276  
You must use IBM FileNet Enterprise Manager to create a FileNet P8 domain and the Global Configuration Data (GCD).
9. “Configuring storage devices for upgrades” on page 279  
When you upgrade from Content Engine version 3.5.2, you must configure your existing file store devices.
10. “Creating the data sources for an object store” on page 282  
Each object store in your site requires its own JDBC data sources. You can configure the data sources by using the Configuration Manager graphical user interface or the command line.
11. “Upgrading Content Search Engine software from version 3.5.2” on page 286  
If you used the full-text search feature (CBR) in version 3.5.2, you upgrade by installing and configuring version 4.5.1 of Content Search Engine (Autonomy K2). After the upgrade, you recreate index areas, called *K2 collections*, to replace the version 3.5.2 content search indexes.
12. “Updating the CFS-IS settings” on page 302  
If Content Federation Services for Image Services (CFS-IS) is in your version 3.5.2 system, then you must enable the Image Services dispatcher. You must also modify the default map between CFS-IS and the object stores in the FileNet P8 domain.
13. “Upgrading Content Engine data” on page 303  
You must upgrade your current Content Engine data (GCD, addons, fixed content devices, object stores, and related information).
14. “Updating the database storage area parameters” on page 328  
After you have upgraded your object stores, you need to initialize the parameter values for the associated database storage areas.
15. “Completing Content Search Engine upgrade from 3.5.2” on page 328  
After you upgrade Content Engine data, you must create new content-search index areas in Enterprise Manager. Then you can enable indexing for designated classes and properties and reindex your stored data. The reindexing process creates new Autonomy K2 collections.
16. “Upgrading Enterprise Manager” on page 331  
If you did not upgrade Enterprise Manager as part of a Content Engine upgrade, you can upgrade Enterprise Manager interactively or silently.

#### Related information



General requirements for all FileNet P8 Platform systems

Check to make sure your software is at the correct fix pack level before you upgrade.

## Completing pre-upgrade Content Engine configuration

You must complete several pre-upgrade procedures to prepare the Content Engine for an upgrade from version 3.5.2.

1. “Verifying that all in-progress event actions have finished” on page 219  
You must verify that all in-progress events have completed for each object store before you begin the upgrade from version 3.5.2.
2. “Verifying that publishing requests have been completed” on page 220  
You must verify that all publishing requests have completed for each object store before you begin the upgrade from version 3.5.2.

3. “Deleting custom subclasses of the PublishRequest object” on page 221  
You must delete any custom subclasses of the PublishRequest class for each object store before you begin the upgrade from version 3.5.2.
4. “Verifying that all in-progress Content Engine transactions involving content files have finished” on page 221  
You must verify that all pending content transactions, indexing requests, and fixed-content migration requests have completed before you begin the upgrade from version 3.5.2. Use the Content Resource Manager utility to view the queues.
5. “Granting directory permissions on file stores (Windows only)” on page 222  
You must give write permission to the root directory of the machine where a version 3.5.2 file store is located to convert the file storage area during upgrade from version 3.5.2.
6. “Renaming storage policies” on page 222  
Check that every storage policy name does not exceed the maximum allowed number of characters. You must shorten the name of any storage policy in version 3.5.2 of IBM FileNet P8 so that it does not exceed 58 characters.
7. “Removing accented characters from file store paths” on page 222  
If you are moving your file stores from Windows to UNIX during your upgrade to version 4.5.1, you must remove any accented characters from the file store path prior to moving the file store.
8. “Determining the CBR-enabled properties in an object store” on page 223  
For each object store to be upgraded, you must determine the associated classes and properties that are currently enabled for content-based retrieval (CBR). You enable these properties after the upgrade is complete.
9. “Preventing name conflicts with reserved words” on page 223  
You must verify that the object store names, custom classes, or custom properties in your current version do not conflict with reserved words before you begin the upgrade from version 3.5.2.
10. “Upgrading IBM InfoSphere Enterprise Records object stores” on page 223  
If you site includes FileNet Records Manager, you must update the FileNet Records Manager data model on each file plan object store (FPOS) before you install Content Engine version 4.5.1.
11. “Running the Content Consistency Checker” on page 224  
Run the Content Consistency Checker to ensure that the documents in the object store database are synchronized with file storage area content.
12. “Moving IBM TotalStorage DR550 fixed content device data” on page 224  
Although IBM TotalStorage DR550 devices have been supported since version 4.5.0 FP2 of Content Engine, there is no upgrade path to move file stores that are on such devices from version 3.5.2 to 4.5.1. If you need to move the content of your DR550 fixed content devices from Content Engine version 3.5.2 to version 4.5.1, contact IBM Support.
13. “Backing up the database” on page 224  
You must back up the database before you begin the upgrade from version 3.5.2.
14. “Stopping and disabling all services related to Content Engine” on page 224  
You must stop and disable all services related to Content Engine on all servers in the FileNet P8 domain before you begin the upgrade from version 3.5.2.

### **Verifying that all in-progress event actions have finished**

You must verify that all in-progress events have completed for each object store before you begin the upgrade from version 3.5.2.

To locate and remove in-progress items from the work queue for the object store:

1. Start Enterprise Manager if it is not already running.
2. In the list view, under the object store icon, right-click the **Search Results** folder and select **New Search**.
3. In the Content Engine Query Builder window, click **Select From Table** → **QueueItem**.
4. Search for unfinished items in the queue or delete unwanted items from the queue:

Option	Description
<b>Search for unfinished items in the queue</b>	<ol style="list-style-type: none"> <li>1. Retain the default settings and click <b>OK</b>.</li> <li>2. Click <b>Yes</b> at the prompt for a WHERE clause. Any remaining event items in the queue are displayed in the Query Status window.</li> </ol>
<b>Remove unwanted items from the queue</b>	<ol style="list-style-type: none"> <li>1. Select the <b>Delete objects</b> check box in the <b>Action</b> tab of the Search dialog box.</li> <li>2. Click <b>OK</b>. Click <b>OK</b> again to confirm the deletion.</li> </ol>

5. Repeat this procedure for each object store in your environment.

### Verifying that publishing requests have been completed

You must verify that all publishing requests have completed for each object store before you begin the upgrade from version 3.5.2.

To verify that publishing requests complete:

1. Start Enterprise Manager if it is not already running.
2. Search for publishing requests in the queue by expanding the **Publishing** folder and clicking **Queue**. Then, click **View** → **All requests**.
3. Verify that the queue (right pane) of publishing requests is empty. If the queue is not empty, wait until the publish requests are processed. If any publish requests are in the In Error state, contact your publishing administrator for the appropriate action to take (such as retrying after correcting the error or just deleting the item).
4. In the list view, under the object store icon, right-click the **Search Results** folder, and choose **New Search**.
5. In the Content Engine Query Builder window, click **Select From Table** → **PublishRequest**.
6. Retain the default settings and click **OK**.
7. Click **Yes** at the prompt for a WHERE clause. Any remaining event items in the queue are displayed in the Query Status window.
8. Remove unwanted items from the queue.
  - a. In the list view, under the object store icon, right-click the **Search Results** folder, and choose **New Search**.
  - b. In the Content Engine Query Builder window, click **Select From Table** → **PublishRequest**.
  - c. Select the **Delete objects** check box in the **Actions** tab of the Search window.
  - d. Click **OK**. Click **OK** again to confirm the deletion.

9. Repeat this procedure for each object store in your environment.

### Deleting custom subclasses of the PublishRequest object

You must delete any custom subclasses of the PublishRequest class for each object store before you begin the upgrade from version 3.5.2.

To delete custom subclasses of the PublishRequest object:

1. Start version 3.5 of IBM FileNet Enterprise Manager.
2. In the left pane of Enterprise Manager, open an object store, and navigate to **Other Classes** → **Custom Object** → **Publish Request**.
3. In the right pane, delete any custom subclasses of Publish Request and any instances of such subclasses.
4. Repeat this procedure for each object store in your environment.
5. Close Enterprise Manager.

### Verifying that all in-progress Content Engine transactions involving content files have finished

You must verify that all pending content transactions, indexing requests, and fixed-content migration requests have completed before you begin the upgrade from version 3.5.2. Use the Content Resource Manager utility to view the queues.

**Important:** All transactions and requests must complete before you upgrade Content Engine. Otherwise, the upgrade will fail.

To verify that all transactions and requests are complete:

1. Start File Store Service if it is not already running on the server where Content Engine is installed.
2. Stop Object Store Service and Content Cache Service.
3. Start the *ce\_install\_path\RMU.exe* utility, where *ce\_install\_path* is the location where the Content Engine software is installed.
4. In the Content Resource Manager Utility window, complete the following steps:
  - a. Navigate to **Statistics** → **Transactions** and note the values of **Total prepared phase 1**, **Total committed**, and **Total aborted**.
  - b. Navigate to **Statistics** → **Can't Do Queue** and note the value of **Current items in the can't do queue**.
  - c. Add the values of **Total committed** and the **Total aborted**. If the sum equals the value of **Total prepared phase 1**, and the value of **Current items in the can't do queue** is zero, then all content transactions are complete.
  - d. Navigate to **Indexing Service** → **Index Control**. If the value of **Current index queue files** is zero, then all pending indexing requests are complete.
  - e. Navigate to **Fixed Content** → **Migration Queuing**. If the value of **Current number in queue** is zero, then all fixed-content migration requests are complete.
5. If all the activities checked are complete, then stop the File Store Service on the server.
6. If any of the activities are not complete, then close the Content Resource Manager utility. Wait several minutes, and then return to Step 1.
7. Repeat this procedure on each server in your environment where Content Engine is installed.

## Granting directory permissions on file stores (Windows only)

You must give write permission to the root directory of the machine where a version 3.5.2 file store is located to convert the file storage area during upgrade from version 3.5.2.

To grant directory permissions:

Give the following users write permission to the root directory of the computer where the version 3.5.2 file store is located:

- The user running Upgrader Tool (*config\_mgr\_user*)
- The user running the application server (*ce\_appserver\_admin*)

If you are running the WebSphere Application Server instance by using the LocalSystem service log-on account and the file stores are located on the same server, then give SYSTEM write permission to the root directory.

If you are running the WebSphere Application Server instance by using the LocalSystem service log-on account, but WebSphere Application Server is remote from the file stores, then change the service log-on account from LocalSystem to an account that would be allowed write access to the file store directories.

### Related concepts

 Specifying IBM FileNet P8 accounts for upgrades

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

## Renaming storage policies

Check that every storage policy name does not exceed the maximum allowed number of characters. You must shorten the name of any storage policy in version 3.5.2 of IBM FileNet P8 so that it does not exceed 58 characters.

To check storage policy names:

1. Start version 3.5.2 of IBM FileNet Enterprise Manager and log in to the P8 domain FileNet P8 domain you are upgrading.
2. For each object store in the left panel, select the Storage Policies node and complete the following substeps for each storage policy:
  - a. Right-click the storage policy node and choose **Properties** from the context menu that opens.
  - b. If the storage policy name has more than 58 characters, change the name so that it does not exceed 58 characters and click **OK**.

## Removing accented characters from file store paths

If you are moving your file stores from Windows to UNIX during your upgrade to version 4.5.1, you must remove any accented characters from the file store path prior to moving the file store.

To remove any accented characters from the file store path:

1. Start the version 3.5.2 Enterprise Manager.
2. Use the Move File Store wizard to change the path for the file store. Do not use any accented characters in the path. See the FileNet P8 Help topic **IBM FileNet P8 documentation** → **System Administration** → **Content Engine Administration** → **Content storage** → **Storage areas** → **File storage areas** → **How to** → **Move a file storage area**



## Determining the CBR-enabled properties in an object store

For each object store to be upgraded, you must determine the associated classes and properties that are currently enabled for content-based retrieval (CBR). You enable these properties after the upgrade is complete.

To determine the classes and properties that are CBR-enabled:

1. Using an RDBMS tool, access the object store database as a user who has appropriate privileges to query the object store tables.
2. Run the following SQL query command on each object store database to determine which properties are enabled for CBR:

```
select p.dbg_class_name, p.dbg_display_name, c.is_cbr_enabled,
p.is_cbr_enabled from ClassDefinition c inner join PropertyDefinition p
on p.parent_id = c.object_id where p.is_cbr_enabled = 1 AND
c.is_cbr_enabled = 0
```

3. Record the results of the query commands. After you upgrade the object stores, you need to run FileNet Enterprise Manager to enable CBR on these properties after you enable CBR on the classes that these properties are associated with.

### Related tasks

“Completing Content Search Engine upgrade from 3.5.2” on page 328

After you upgrade Content Engine data, you must create new content-search index areas in Enterprise Manager. Then you can enable indexing for designated classes and properties and reindex your stored data. The reindexing process creates new Autonomy K2 collections.

## Preventing name conflicts with reserved words

You must verify that the object store names, custom classes, or custom properties in your current version do not conflict with reserved words before you begin the upgrade from version 3.5.2.

Verify that your custom classes and properties do not conflict with the reserved words listed in "New Content Engine classes and properties" in *Plan and Prepare Your Environment for IBM FileNet P8* that describes how you must change any custom class or custom property names in your existing object stores. If you have previously defined any classes or properties in a version 3.5.2 object store with symbolic names that are the same as any of the reserved class or property symbolic names, the upgrade tool detects the naming conflicts and requires you to change your class or property names before it upgrades the object store to version 4.5.1. Therefore, you must resolve conflicts between your version 3.5.2 symbolic names and the version 4.0 and 4.5 symbolic names

### Related concepts

 Upgrade tasks

For details on the necessary steps to prepare for an upgrade, see *Plan and Prepare Your Environment for IBM FileNet P8*.

## Upgrading IBM InfoSphere Enterprise Records object stores

If your site includes FileNet Records Manager, you must update the FileNet Records Manager data model on each file plan object store (FPOS) before you install Content Engine version 4.5.1.

To complete and confirm your IBM FileNet P8 Platform upgrade, you must update at least one object store. If your configuration contains only FileNet Records Manager object stores, you must update at least one of the object stores or create a non-Records Manager object store prior to upgrading and use that object store to confirm the upgrade.



Run the RM37PreUpgrader tool. See the topic "Prepare to Upgrade Object Stores" in *IBM FileNet Records Manager Installation and Upgrade Guide*

## Running the Content Consistency Checker

Run the Content Consistency Checker to ensure that the documents in the object store database are synchronized with file storage area content.

For information about the Content Consistency Checker, see the IBM FileNet P8 Help topic **FileNet P8 Administration** → **Content Engine Administration** → **Content storage** → **Content Consistency Checker Overview**.

## Moving IBM TotalStorage DR550 fixed content device data

Although IBM TotalStorage DR550 devices have been supported since version 4.5.0 FP2 of Content Engine, there is no upgrade path to move file stores that are on such devices from version 3.5.2 to 4.5.1. If you need to move the content of your DR550 fixed content devices from Content Engine version 3.5.2 to version 4.5.1, contact IBM Support.

## Backing up the database

You must back up the database before you begin the upgrade from version 3.5.2.

1. Use your existing database backup solution to back up each of the Content Engine object store databases.
2. Make a backup copy of the version 3.5.2 Global Configuration Data GCD file. The default location is C:\Program Files\FileNet\Content Engine\sysconfig\sysinit\sysinit.dat.

## Stopping and disabling all services related to Content Engine

You must stop and disable all services related to Content Engine on all servers in the FileNet P8 domain before you begin the upgrade from version 3.5.2.

1. Log on with local administrator permissions to the server where Content Engine version 3.5.2 is installed.
2. Stop and disable the following services:
  - Apache2
  - Content Engine Content Cache Service
  - Content Engine File Store Service
  - Content Engine Object Store Service
  - FileNet Publishing HTML Plug-in Service
  - FileNet Publishing PDF Plug-in Service
  - Process Services Manager
  - Wasp Server for Java
  - FileNet P8 CFS Server for Image Services
3. Right-click the Apache services monitor in the Windows system tray, and click **Exit**.
4. Repeat this procedure on each Content Engine server in your FileNet P8 domain.

## Upgrading Content Engine and related client software

If you are upgrading from Content Engine version 3.5.2 on Windows, you can upgrade and continue to use Windows, or you can migrate your Content Engine to UNIX.

In either case, you must prepare the Content Engine application for deployment and then upgrade the object store data.

Migrating your Content Engine version 3.5.2 on a Windows server to Content Engine version 4.5.1 on UNIX requires a new installation of Content Engine on your UNIX machine. You also need access to a Windows machine to install and run IBM FileNet Enterprise Manager and the Content Engine Upgrader tool.

It is a best practice to retain a Windows machine where version 3.5.2 of IBM FileNet Enterprise Manager is installed. If you use the Content Engine Upgrader tool, you need access to this Windows-based tool. If you use Content Engine Web Upgrade Tool, you can browse to it only from a machine where version 8.0 of Microsoft Internet Explorer is installed.

1. "Installing or upgrading Content Engine"  
You can install or upgrade Content Engine, Configuration Manager, .NET Clients (including IBM FileNet Enterprise Manager), Content Engine Upgrader, and FileNet Deployment Manager either interactively or silently.
2. "Installing Content Engine software updates" on page 228  
You must apply any updates, fix packs, or interim fixes for the Content Engine software that have been released.
3. "Installing the latest Content Search Engine Client files on Content Engine servers" on page 228  
If your environment includes Content Search Engine, you must install the files that Content Engine uses to communicate with Content Search Engine.
4. "Installing the latest Process Engine client files on Content Engine servers" on page 231  
You must install the Process Engine Client files on all application server machines where Content Engine Server is deployed.

## Installing or upgrading Content Engine

You can install or upgrade Content Engine, Configuration Manager, .NET Clients (including IBM FileNet Enterprise Manager), Content Engine Upgrader, and FileNet Deployment Manager either interactively or silently.

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

If you are installing in a managed environment, then the application server must be the Deployment Manager node for WebSphere Application Server or the Administrator node for Oracle WebLogic Server.

If the Content Engine installer detects an existing Content Engine installation, the software will be upgraded.

Some Content Engine components must be installed on a Windows operating system. The following table lists the Content Engine components and the required operating system.

*Table 18. Content Engine components*

Component	Required Platform
Content Engine Server	UNIX or Windows
Configuration Manager	UNIX or Windows
.NET Clients (including IBM FileNet Enterprise Manager)	Windows only

Table 18. Content Engine components (continued)

Component	Required Platform
Content Engine Upgrader	Windows only
FileNet Deployment Manager	Windows only

Install the .NET Clients software only on machines where you intend to run either the Enterprise Manager administrative client or a customized client application.

**Important:** You must keep one running version of Enterprise Manager version 3.5.2 until after you upgrade the Content Engine data. You must use Enterprise Manager version 3.5.2 to prepare your version 3.5.2 object stores for the Content Engine data upgrade.

The Content Engine Upgrader tool or Content Engine Web Upgrade Tool is required to upgrade Content Engine and Content Search Engine data from version 3.5.2.

The FileNet Deployment Manager is an optional component that you can use to deploy test systems into full production. See the IBM FileNet P8 help topic **Application Deployment** → **Get Started with FileNet Deployment Manager** for details.

You can install or upgrade Content Engine interactively or silently.


“Installing Content Engine interactively”

You can interactively install or upgrade Content Engine, Configuration Manager, .NET Clients (including IBM FileNet Enterprise Manager), Content Engine Upgrader, and IBM FileNet Deployment Manager.

“Installing Content Engine silently” on page 227

You can silently install or upgrade Content Engine, Configuration Manager, .NET Clients (including IBM FileNet Enterprise Manager), Content Engine Upgrader, and IBM FileNet Deployment Manager.

#### 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

“Configuring storage devices for migration to UNIX” on page 279

When you upgrade from Content Engine version 3.5.2 and migrate to a UNIX server, you must prepare the UNIX server to mount your existing file store devices.

#### Installing Content Engine interactively:

You can interactively install or upgrade Content Engine, Configuration Manager, .NET Clients (including IBM FileNet Enterprise Manager), Content Engine Upgrader, and IBM FileNet Deployment Manager.

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

**Important:** You must keep one running version of Enterprise Manager version 3.5 until after you upgrade the Content Engine data. You must use Enterprise Manager version 3.5 to prepare your version 3.5 object stores for the Content Engine Upgrader tool.

To install Content 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 Engine values, filter by **CE Installer** in the **Installation or Configuration Program** column.

2. Log on as *ce\_install\_user* to the application server machine where you are going to install Content Engine software.
3. Navigate to the Content 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
AIX	P8CE-4.5.1-AIX.BIN
HPUX	P8CE-4.5.1-HPUX.BIN
HPUXi	P8CE-4.5.1-HPUXI.BIN
Linux	P8CE-4.5.1-LINUX.BIN
Linux on System z	P8CE-4.5.1-ZLINUX.BIN
Solaris	P8CE-4.5.1-SOL.BIN
Windows	P8CE-4.5.1-WIN.EXE

5. When the installation completes, click **Done** and check for errors in the Content Engine *ce\_install\_path/ce\_install\_log\_4\_5\_1.txt* error log file, where *ce\_install\_path* is the location where Content Engine is installed.

### Installing Content Engine silently:

You can silently install or upgrade Content Engine, Configuration Manager, .NET Clients (including IBM FileNet Enterprise Manager), Content Engine Upgrader, and IBM FileNet Deployment Manager.

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

**Important:** You must keep one running version of Enterprise Manager version 3.5.2 until after you upgrade the Content Engine data. You must use Enterprise Manager version 3.5.2 to prepare your version 3.5.2 object stores for the Content Engine Upgrader tool.

To install Content 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 Engine values, filter by **CE Installer** in the **Installation or Configuration Program** column.

2. Log on as *ce\_install\_user* to the application server machine where you are going to install Content Engine software.

3. Navigate to the Content 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
AIX	P8CE-4.5.1-AIX.BIN -f CE_silent_install.txt -i silent
HPUX	P8CE-4.5.1-HPUX.BIN -f CE_silent_install.txt -i silent
HPUXi	P8CE-4.5.1-HPUXI.BIN -f CE_silent_install.txt -i silent
Linux	P8CE-4.5.1-LINUX.BIN -f CE_silent_install.txt -i silent
Linux on System z	P8CE-4.5.1-ZLINUX.BIN -f CE_silent_install.txt -i silent
Solaris	P8CE-4.5.1-SOL.BIN -f CE_silent_install.txt -i silent
Windows	P8CE-4.5.1-WIN.EXE -f CE_silent_install.txt -i silent

6. When the installation completes, check for errors in the Content Engine error log file `ce_install_path/ce_install_log_4_5_1.txt`, where `ce_install_path` is the location where Content Engine is installed.

### Installing Content Engine software updates

You must apply any updates, fix packs, or interim fixes for the Content Engine software that have been released.

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

To install the Content Engine software updates:

Open the readmes for the Content Engine software updates, and perform the installation procedures in the readmes on each Content Engine instance.

### Installing the latest Content Search Engine Client files on Content Engine servers

If your environment includes Content Search Engine, you must install the files that Content Engine uses to communicate with Content Search Engine.

**Important:** With the initial release of Content Engine 4.5.1, the Content Search Engine 4.5.1 client files are included. Therefore, you are not required to manually install these client files on a new Content Engine server. However, if fix packs of these client files become available, install them manually before you use Configuration Manager to configure and deploy Content Engine. For instructions on how to obtain the latest Content Search Engine Client software updates, access the IBM FileNet P8 Platform support site.

You can manually install Content Search Engine Client files either interactively or silently:

“Installing Content Search Engine Client files interactively”

You can install the Content Search Engine Client files interactively by running the installation program on all application server machines where Content Engine Server is installed.

“Installing Content Search Engine Client files silently” on page 230

You can install the Content Search Engine Client files silently by editing a silent input file and running the installation program from a command line. You must install Content Search Engine Client files on all application server machines where Content Engine Server is installed.

**Installing Content Search Engine Client files interactively:**

You can install the Content Search Engine Client files interactively by running the installation program on all application server machines where Content Engine Server is installed.

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

To install Content Search Engine Client 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 Content Search Engine Client values, filter by **CSE Client Installer** in the **Installation or Configuration Program** column.

2. To download the latest software updates, and to determine which of these updates might be required for use with other components and expansion products, contact your service representative.
3. On the machine where Content Engine is to be deployed, log on as *ce\_install\_user*.
4. Locate the Content Search Engine Client installation software. It must be the same version as your Content Search Engine Server software. You must install Content Search Engine and Content Engine software on the same operating system. For example, if Content Engine runs on Windows, locate the Content Search Engine Client installation software that runs on Windows.
5. Start the installation program.

Operating System	Install Program
AIX	P8CSE-CLIENT-4.5.1-AIX.BIN
HP-UX	P8CSE-CLIENT-4.5.1-HPUX.BIN
HP-UXi	P8CSE-CLIENT-4.5.1-HPUXi.BIN
Linux	P8CSE-CLIENT-4.5.1-LINUX.BIN
Linux on System z	P8CSE-CLIENT-4.5.1-ZLINUX.BIN
Solaris	P8CSE-CLIENT-4.5.1-SOL.BIN
Windows	P8CSE-CLIENT-4.5.1-WIN.EXE

6. Complete the Content Search Engine Client installation screens by using the values in your worksheet.
7. Review the following Content Search Engine Client log files:
  - Windows - *cse\_client\_install\_path\CSEClient\_install\_log\_4.5.1.0.log*
  - UNIX - *cse\_client\_install\_path/CSEClient\_install\_log\_4.5.1.0.log*

## 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 Content Search Engine Client files silently:

You can install the Content Search Engine Client files silently by editing a silent input file and running the installation program from a command line. You must install Content Search Engine Client files on all application server machines where Content Engine Server is installed.

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

To install Content Search Engine Client 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 Content Search Engine Client values, filter by **CSE Client Installer** in the **Installation or Configuration Program** column.

2. To download the latest software updates, and to determine which of these updates might be required for use with other components and expansion products, contact your service representative.
3. On the machine where Content Engine is to be deployed, log on as *ce\_install\_user*.
4. Locate the Content Search Engine Client installation software. It must be the same version as your Content Search Engine Server software. You must install Content Search Engine and Content Engine software on the same operating system. For example, if Content Engine runs on Windows, locate the Content Search Engine Client installation software that runs on Windows.
5. Locate the *CSE\_silent\_install.txt* file within the directory that contains the Content Search Engine Client installation software, and edit the file to specify the location where you want to install the Content Search Engine Client files.

The default installation paths are as follows:

**UNIX** /opt/IBM/FileNet/ContentEngine/CSEClient

#### Windows

C:\Program Files\IBM\FileNet\ContentEngine\CSEClient

6. Start the silent installation of Content Search Engine Client files by running the following command.

Operating System	Install Program
AIX	P8CSE-CLIENT-4.5.1-AIX.BIN -f CSEClient_silent_install.txt -i silent
HP-UX	P8CSE-CLIENT-4.5.1-HPUX.BIN -f CSEClient_silent_install.txt -i silent
HP-UXi	P8CSE-CLIENT-4.5.1-HPUXi.BIN -f CSEClient_silent_install.txt -i silent
Linux	P8CSE-CLIENT-4.5.1-LINUX.BIN -f CSEClient_silent_install.txt -i silent




Operating System	Install Program
Linux on System z	P8CSE-CLIENT-4.5.1-ZLINUX.BIN -f CSEClient_silent_install.txt -i silent
Solaris	P8CSE-CLIENT-4.5.1-SOL.BIN -f CSEClient_silent_install.txt -i silent
Windows	P8CSE-CLIENT-4.5.1-WIN.EXE -f CSEClient_silent_install.txt -i silent

7. Review the following Content Search Engine log files:

- Windows - *cse\_client\_install\_path*\  
CSEClient\_install\_log\_release\_number.log
- UNIX - *cse\_client\_install\_path*/  
CSEClient\_install\_log\_release\_number.log

### 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 Process Engine client files on Content Engine servers

You must install the Process Engine Client files on all application server machines where Content Engine Server is deployed.

“Upgrading the latest Process Engine client files on Content Engine servers interactively”

The upgrade wizard provides an interactive way to upgrade the Process Engine Client files. You can use the values you collected on your worksheet to fill in the required value for each field on the wizard screens.

“Upgrading the latest Process Engine client files on Content Engine servers silently” on page 232

You can upgrade the Process Engine Client software on the Content Engine server by using a silent input text file and running the upgrade program from the command line. Use the values in your installation and upgrade worksheet to edit the silent input text file before you run the upgrade.

### Upgrading the latest Process Engine client files on Content Engine servers interactively:

The upgrade wizard provides an interactive way to upgrade the Process Engine Client files. You can use the values you collected on your worksheet to fill in the required value for each field on the wizard screens.

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

To upgrade the Process Engine Client 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 Content Engine values, filter by **PE Client Installer** in the **Installation or Configuration Program** column.


2. To download the latest software updates, and to determine which of these updates might be required for use with other components and expansion products, contact your service representative.

3. On the machine where Content Engine is to be deployed, log on as *ce\_upgrade\_user*.
4. Access the Process Engine Client install software from the Process Engine installation software. The version of the install software must match the version of Process Engine.
5. Expand the (TAR or ZIP) Process Engine Client install software.
6. Shut down all instances of Enterprise Manager and any other Content Engine client applications, such as Application Engine.
7. Run the command for the installation program according to your operating system.

Operating System	Install Program
AIX	P8PE-CLIENT-4.5.1-AIX.BIN
HPUX	P8PE-CLIENT-4.5.1-HPUX.BIN
HPUXi	P8PE-CLIENT-4.5.1-HPUXI.BIN
Linux	P8PE-CLIENT-4.5.1-LINUX.BIN
Solaris	P8PE-CLIENT-4.5.1-SOL.BIN
Windows	P8PE-CLIENT-4.5.1-WIN.EXE
zLinux	P8PE-CLIENT-4.5.1-ZLINUX.BIN

8. Complete the Process Engine client install screens.

#### 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*.

#### Upgrading the latest Process Engine client files on Content Engine servers silently:

You can upgrade the Process Engine Client software on the Content Engine server by using a silent input text file and running the upgrade program from the command line. Use the values in your installation and upgrade worksheet to edit the silent input text file before you run the upgrade.

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

To install the Process Engine Client files 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 **PE Client Installer** in the **Installation or Configuration Program** column.


2. To download the latest software updates, and to determine which of these updates might be required for use with other components and expansion products, contact your service representative.
3. On the machine where Content Engine is to be deployed, log on as *ce\_upgrade\_user*.
4. Access the Process Engine Client install software from the Process Engine installation software. The version of the install software must match the version of Process Engine.

5. Expand the (TAR or ZIP) Process Engine Client install software.
6. Shut down all instances of Enterprise Manager and any other Content Engine client applications, such as Application Engine.
7. In the expanded install software, open the file PEClient\_silent\_install.txt and edit it as follows: Change the Variable\_CheckboxCE line to the following line:
 

```
-V Variable_CheckboxCE="true"
```
8. Save your edits.
9. Run one of the commands in the following table to perform the silent install:

Operating System	Install Program
AIX	P8PE-CLIENT-4.5.1-AIX.BIN -silent -options "PEClient_silent_install.txt"
HPUX	P8PE-CLIENT-4.5.1-HPUX.BIN -silent -options "PEClient_silent_install.txt"
HPUXi	P8PE-CLIENT-4.5.1-HPUXI.BIN -silent -options "PEClient_silent_install.txt"
Linux	P8PE-CLIENT-4.5.1-LINUX.BIN -silent -options "PEClient_silent_install.txt"
Solaris	P8PE-CLIENT-4.5.1-SOL.BIN -silent -options "PEClient_silent_install.txt"
Windows	P8PE-CLIENT-4.5.1-WIN.EXE -silent -options "PEClient_silent_install.txt"
Linux on System z	P8PE-CLIENT-4.5.1-ZLINUX.BIN -silent -options "PEClient_silent_install.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 Content Engine

You can configure and deploy all of your Content Engine instances by using Configuration Manager. A single Content 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 Engine application environment, then you apply the settings by running the configuration tasks, and then you 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 Engine instance:

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

- Content Engine bootstrap properties

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

- (WebSphere Application Server only) For best results, configure no more than one Content Engine instance in a WebSphere profile.
- If you need an accessible software version of Configuration Manager for people with disabilities, use the command-line version of Configuration Manager.
- If your system is HP-RISC, use the command-line version of Configuration Manager.
- If your system is Novell SUSE Linux Enterprise 9, use the command-line version of Configuration Manager.
- 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 complete the tasks on the initial server, you copy the EAR file with the bootstrap settings to the additional servers.

Begin the configuration process by ensuring that you have the necessary operating system permissions to use Configuration Manager.

To grant permissions to the Configuration Manager user:

1. Log on as *ce\_install\_user* to the server where you installed Content Engine.
2. Grant permissions to the *config\_mgr\_user* user for the executable file that you intend to use:

Option	Description
UNIX - graphical user interface	Grant execute permission to configmgr
UNIX - command line	Grant execute permission to configmgr_cl
Windows - graphical user interface	Grant read and execute permission to configmgr.exe
Windows - command line	Grant read and execute permission to configmgr_cl.exe

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 Engine server and log on again as *config\_mgr\_user*.
  1. “Configuring Content Engine instances by using the graphical user interface”  
You can use the graphical user interface version of Configuration Manager to configure and deploy a Content Engine application instance on an application server.
  2. “Configuring instances by using the command line” on page 242  
You can configure a Content Engine instance on a web application server by using the command-line version of Configuration Manager.

### Configuring Content Engine instances by using the graphical user interface

You can use the graphical user interface version of Configuration Manager to configure and deploy a Content 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 Engine application
- The directory service provider (LDAP) settings
- The Content 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 Login Modules, Configure LDAP properties, and Configure Bootstrap 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 Configuration Manager”  
You can start the graphical interface version of Configuration Manager to configure a Content Engine application instance on a web application server.
2. “Changing the password save preference” on page 236  
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 237  
Configuration Manager stores your settings for deploying a Content 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 Engine bootstrap settings, and the application deployment settings. You must create a new profile for each Content Engine instance that you are configuring.
4. “Configuring the Global Configuration Data JDBC data source settings” on page 238  
You must provide property information about the JDBC data sources for the Global Configuration Data (GCD) database. Content Engine uses the data source information to connect to and update the GCD database.
5. “Configuring the login modules (WebSphere and JBoss only)” on page 239  
You must configure the login modules for the Content Engine application. The login modules provide authentication information for the Content Engine application.
6. “Configuring the directory service provider (LDAP) settings” on page 240  
You must configure the directory service provider (LDAP) settings. The directory service provider (LDAP) settings define the directory service and the users and groups that Content Engine uses for authentication.
7. “Configuring the bootstrap settings” on page 241  
You must configure the bootstrap settings. The bootstrap information is needed for creating the Global Configuration Data (GCD) and for starting Content Engine.

### **Starting Configuration Manager:**

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

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 Engine:

Option	Description
UNIX	Run this command: <code>ce_install_path/tools/configure/configmgr</code>
Windows	Perform one of the following actions: <ul style="list-style-type: none"> <li>• Double-click the <b>FileNet Configuration Manager</b> desktop shortcut.</li> <li>• Click <b>Start</b> → <b>All Programs</b> → <b>IBM FileNet P8 Platform</b> → <b>FileNet Configuration Manager</b>.</li> <li>• Run the following command: <code>ce_install_path\tools\configure\configmgr.exe</code></li> </ul>

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.

#### Related tasks

“Deploying upgraded instances by using the graphical user interface” on page 259  
You can deploy an upgraded Content Engine Server instance on a web application server by using the graphical user interface version of Configuration Manager. Deploying makes the Content Engine application available for use.

#### 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, you must specify any passwords required by the tasks and for the application server properties before you run the tasks; otherwise, the tasks won't 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 <b>Save all passwords to file when saving a task or profile</b> check box.
To prevent writing passwords to file	Clear the <b>Save all passwords to file when saving a task or profile</b> check box.

3. Click **OK**.

## Creating a new configuration profile:

Configuration Manager stores your settings for deploying a Content 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 Engine bootstrap settings, and the application deployment settings. You must create a new profile for each Content 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 Engine is installed. For more information on profiles, see “Configuration profile concepts” on page 532.

**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.
4. 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*.

## Related tasks

“Configuration Manager user interface reference” on page 538

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content 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.

## Configuring the Global Configuration Data JDBC data source settings:

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

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

*Table 19. Required application server state*

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

To configure the JDBC 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 GCD JDBC Data Sources** 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 GCD JDBC Data Sources** in the profile pane and select **Edit Selected Task**.
4. Enter the property values for your database by using the values in your worksheet.
5. 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.
6. Select **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 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*.

#### Related tasks

“Configuration Manager user interface reference” on page 538

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content 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.

#### Configuring the login modules (WebSphere and JBoss only):

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

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


*Table 20. Required application server state*

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

To configure the login module settings:

1. If your configuration profile is not open in Configuration Manager, open the profile.
2. 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 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

“Configuration Manager user interface reference” on page 538

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content 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.

## Configuring the directory service provider (LDAP) settings:

You must configure the directory service provider (LDAP) settings. The directory service provider (LDAP) settings define the directory service and the users and groups that Content Engine uses for authentication.

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

If you plan to configure Content 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 **System Administration** → **Enterprise-wide Administration** → **FileNet P8 Security** → **How to...** → **Configuration Content Engine to use e-mail or UPN for login**.

**Restriction:** JBoss Application Server only. Do not use Configuration Manager to configure multiple LDAP realms. Use IBM FileNet Enterprise Manager to configure multiple realms, as instructed in the IBM FileNet P8 help topic **System Administration** → **Enterprise-wide Administration** → **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 **File** → **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.

Oracle WebLogic Server only. When you run the **Configure LDAP** task, the `weblogic.security.providers.authentication.DefaultAuthenticator.ControlFlag` value is set to `SUFFICIENT` for authenticating users.

### 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

“Configuration Manager user interface reference” on page 538

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content 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.

### Configuring the bootstrap settings:

You must configure the bootstrap settings. The bootstrap information is needed for creating the Global Configuration Data (GCD) and for starting Content Engine.

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 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** 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. Optional: Click **Verify Bootstrap Information** to display the bootstrap information from the modified EAR file.
7. Click **File** → **Save** to save your changes.

8. 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 Properties (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.
9. Apply the bootstrap property settings by right-clicking **Configure bootstrap properties** 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.
10. Close the Configure Bootstrap Properties 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 each additional Content Engine server.

*install\_dir*

The location where Content 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:** Only run the **Configure bootstrap properties** task 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*.

### Related tasks

“Configuration Manager user interface reference” on page 538

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content 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.

## Configuring instances by using the command line

You can configure a Content 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 Data (GCD) data source JDBC data source settings, the login modules for the Content Engine application, the directory service provider (LDAP) settings, and the Content 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 Engine application. If you are deploying multiple Content 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 Engine instance”  
The configuration XML files contain the properties and values for the various configuration tasks. From the command line, you can generate all the XML files at the same time, or you can generate a single configuration XML file at a time.
2. “Editing the configuration XML files for a Content Engine instance” on page 250  
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.
3. “Running the configuration XML files” on page 252  
Running the configuration XML files applies the settings. You use the **execute** command to apply your configuration settings from the command line.
4. “Checking the completion status of Content Engine configuration tasks” on page 257  
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 Engine instance:**

The configuration XML files contain the properties and values for the various configuration tasks. From the command line, you can generate all 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 Engine instance.

*Table 21. Configuration XML files*

<b>File Name</b>	<b>Description</b>
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 Data (GCD) and starting Content Engine.

Table 21. Configuration XML files (continued)

File Name	Description
configurejdbcgcd.xml	Settings for configuring JDBC connections to the databases used by Content Engine. You must generate, edit, and run the configure the JDBC task once for the data sources for the Global Configuration Data (GCD) and then again for the data sources for each object store. For information about creating the additional data sources for the object store, see “Creating the data sources by using the command line” on page 74.
configurejdbcgos.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	
configureloginmodules.xml	Settings for creating the application server login modules for Content Engine.

You must eventually generate each of the required configuration XML files to configure a Content 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 Engine at the same time with a single command.

“Generating one configuration XML file at a time (WebSphere)” on page 246

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

“Generating one configuration XML file at a time (WebLogic or JBoss)” on page 248

From the command line, you can generate each of the required configuration XML files for Content 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 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 application 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 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
```

#### Oracle WebLogic Server or JBoss Application Server

```
configmgr_cl generateconfig -appserver app_server_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` or `configurejdbcos` option. This parameter specifies the type of database to be used by Content 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 Engine uses for authenticating users and must be `activedirectory`, `adam`, `edirectory`, `oid`, `sunjava`, 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 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 Engine deployment. The value must be `standard`, `cluster`, or `netdeploy` (network deployment).

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

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

To generate a single configuration XML file:

1. Log on to the application server as *config\_mgr\_user*, which is 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 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 Engine uses for authenticating users and must be *activedirectory*, *adam*, *edirectory*, *oid*, *sunjava*, 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 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 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.

*Generating one configuration XML file at a time (WebLogic or JBoss):*

From the command line, you can generate each of the required configuration XML files for Content 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 Data (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.

To generate a single configuration XML file:

1. Log on to the application server as `config_mgr_user`, which is 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.

**Oracle WebLogic Server or JBoss Application Server only. Generate the `configurebootstrap.xml` file for the `configurebootstrap` task:**

```
configmgr_cl generateconfig -appserver app_server_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
 -db db_type -task configurejdbcgcd -profile myprofile
```

Generate the `configurejdbcos.n.xml` file for the `configurejdbcos` task for the data sources for a single object store:

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

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

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

**JBoss only.** Generate the `configureloginmodules.xml` file for the `configureloginmodules` task:

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

where:

**-appserver** *appserver\_name*

**-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 files by using the `configurejdbcgcd` or `configurejdbcos` option. This parameter specifies the type of database to be used by Content 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 Engine uses for authenticating users and must be `activedirectory`, `adam`, `edirectory`, `oid`, `sunjava`, 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 operation for the profile and must be `new`, `modify`, or `upgrade`.

**-profile** *myprofile*

The **-profile** *myprofile* parameter specifies the profile to use. Use one of the following values for *myprofile*:

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

#### **Editing the configuration XML files for a Content 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.

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 each 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 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 Data (GCD)
- 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 Global Configuration Data (GCD) database, 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 database.
5. Save your edits and close the XML file.
6. Optional: Add encrypted passwords to the XML files by running the `storepasswords` command.

- a. Enter the following command on one line:

```
configmgr_c1 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 Engine settings affected by the task.

Table 22. *task\_type* values

Task	Configuration file	Description
omitted	<code>applicationserver.xml</code> <code>configurebootstrap.xml</code> <code>configurejdbc.xml</code> <code>configureldap.xml</code> <code>deployapplication.xml</code>	When you omit the <code>-task task_type</code> 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.
<code>configurebootstrap</code>	<code>configurebootstrap.xml</code>	Encrypts the password for the <code>BootstrapPassword</code> property that is used to create the Global Configuration Data and to start Content Engine.
<code>configurejdbcgcd</code>	<code>configurejdbcgcd.xml</code>	Encrypts the password for the <code>DatabasePassword</code> property that Content Engine uses to access the GCD database.
<code>configurejdbcos</code>	<code>configurejdbcos.xml</code> <code>configurejdbcos.n.xml</code> , where <i>n</i> is an integer starting with 2	Encrypts the password for the <code>DatabasePassword</code> property that Content Engine uses to access the object store database.  If you have more than one <code>configurejdbcos.n.xml</code> file, run the command for each task file.



Table 22. *task\_type* values (continued)

Task	Configuration file	Description
configureldap	configureldap.xml  configureldap. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Encrypts the password for the LDAPBindPassword property that Content Engine uses to connect to the directory server for authenticating Content Engine users.  If you have more than one configureldap. <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 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 edit 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 535 for more information.

To run the configuration XML files:

1. Start or stop the application server.

Option	Description
<b>WebSphere Application Server</b>	Start the application server if it is not already running.
<b>JBoss Application Server</b>	Stop the application server.
<b>Oracle WebLogic Server</b>	Start the application server 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 of the configuration XML files at the same time”

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

“Running one configuration XML file at a time” on page 254

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 Engine configuration.

*Running all of the configuration XML files at the same time:*

From the command line, you can run all of the required configuration XML files for Content Engine at the same time with a single command. Any configuration XML file that has the <TaskEnabled> 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 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 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 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 each additional Content Engine server.

*install\_dir*

The location where Content 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.

Oracle WebLogic Server only. When you run all the tasks, the `weblogic.security.providers.authentication.DefaultAuthenticator.ControlFlag` value is set to `SUFFICIENT` for authenticating users.

*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 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 535 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 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 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 Engine server.

- Configure the JDBC Data Sources for the Global Configuration Data (GCD) database 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.  
Oracle WebLogic Server only. When you run the task using the `configureldap` option, the `weblogic.security.providers.authentication.DefaultAuthenticator.ControlFlag` value is set to `SUFFICIENT` for authenticating users.
- 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 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 task_file_name
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 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 Global Configuration Data (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 each additional Content Engine server.

*install\_dir*

The location where Content 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 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 23. 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 258

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 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 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 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 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 2 on page 258 as needed to check status on one of the other configuration XML files.

The task execution status messages are displayed.

## Deploying upgraded Content Engine instances

You must deploy the upgraded Content Engine on the web application server. Deploying makes the Content Engine application available for use.

**Restriction:** Use the command-line version of Configuration Manager if any of these conditions is true:

- Your system is HP-RISC. You can configure Content Engine only with the command line.
- Your system is Novell SUSE Linux Enterprise 9. You can configure Content Engine only with the command line.
- You need an accessible software version of Configuration Manager for people with disabilities to use.

“Deploying upgraded instances by using the graphical user interface”

You can deploy an upgraded Content Engine Server instance on a web application server by using the graphical user interface version of Configuration Manager. Deploying makes the Content Engine application available for use.

“Deploying upgraded instances by using the command line” on page 261

You can deploy an upgraded Content Engine instance on a web application server by using the command-line version of Configuration Manager. Deploying makes the Content Engine application available for use.

### Deploying upgraded instances by using the graphical user interface

You can deploy an upgraded Content Engine Server instance on a web application server by using the graphical user interface version of Configuration Manager. Deploying makes the Content Engine application available for use.

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

Make sure that the application server is running or stopped, depending on its type:

Table 24. Required Application Server State

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

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

To deploy Content 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 Engine 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*, the Configuration Manager user.
3. Start Configuration Manager. See “Starting Configuration Manager” on page 235.
4. Select **File** → **Open Configuration Profile**, and use the information in your worksheet to specify the values for the parameters in the wizard screens.
5. In the Open Configuration Profile wizard, enter the path to the profile for the Content Engine instance, and then click **Finish**.
6. Right-click the **Deploy Application** task in the profile pane (left pane), and select **Edit Selected Task**.
7. Provide the property values for your deployment by using the values in your worksheet.
8. Select **File** → **Save**.
9. Enable the task. By default, the **Deploy Application** task is disabled. 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.
10. Right-click the **Deploy Application** task in the left pane, and select **Run Task**. Running the deploy task might take a few minutes. The task execution status messages are displayed in the Console pane below the deploy application properties.
11. Return to the parent topic and complete the task.

## Related concepts

 Accounts for Content Engine upgrade

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*.

## Related tasks

“Starting Configuration Manager” on page 235

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

## Deploying upgraded instances by using the command line

You can deploy an upgraded Content Engine instance on a web application server by using the command-line version of Configuration Manager. Deploying makes the Content Engine application available for use.

Ensure that the application server is running or stopped:

Table 25. Required Application Server State

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

See “Configuration Manager command-line reference” on page 555 for syntax details.

To deploy a Content Engine instance from the command line:

1. Log on to the application server machine as the *config\_mgr\_user* user, which is the Configuration Manager user.
2. If you upgraded the version of your application server, or if you moved it to a new directory or device and then redeployed Content Engine before upgrading Content Engine to version 4.5.1 from version 4.0.1 or 4.5.0, perform the following substeps:
  - a. Open the *applicationserver.xml* file for editing.
  - b. Correct any obsolete parameter values for your application server type.
  - c. Save your edits.
3. Set the current directory to *ce\_install\_path/tools/configure*, where *ce\_install\_path* is the path where you installed Content Engine.
4. Run the following command to apply the settings in the *deployapplication.xml* file:

```
configmgr execute -task deployapplication -profile myprofile
```

where 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 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".

5. Optional: Run the following command to check the completion status of the DeployApplication task.  

```
configmgr checkstatus -task deployapplication -profile myprofile
```
6. Repeat this procedure as needed to deploy any additional Content Engine instances.

### 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

“Configuration Manager user interface reference” on page 538

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content 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.

## Installing storage device source files

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

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

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 and adding native API library paths (WebLogic)” on page 264

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 and adding native API library paths (JBoss)” on page 267

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 269

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

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

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

1. "Installing Tivoli Storage Manager client"  
Install the Tivoli Storage Manager client software on each application server where Content Engine is deployed.
2. "Copying the Tivoli Storage Manager API library files to additional servers"  
If you are running a Content Engine server farm, the Tivoli Storage Manager API libraries must be on each server in the farm.
3. "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.

### Installing Tivoli Storage Manager client:

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

1. Download the Tivoli Storage Manager client software from the IBM Support site at <http://www-01.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 fixed content device in FileNet Enterprise Manager. If you are installing Tivoli Storage Manager client on multiple UNIX hosts, the installation path must be the same on each host. On AIX, install Tivoli Storage Manager client at `/usr/tivoli/tsm/client/ba/bin`.

### Copying the Tivoli Storage Manager API library files to additional servers:

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

Copy the entire `tsm100` directory structure from the Content 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
UNIX	<code>/opt/IBM/FileNet/ContentEngine/tsm100</code>
Windows	<code>C:\Program Files\IBM\FileNet\ContentEngine\tsm100</code>

### 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.

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. For the detailed procedure on creating the shared library, visit <http://www.ibm.com/software/webservers/appserv/was/library/>.
  - 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.

### Installing Tivoli Storage Manager client and adding native API library paths (WebLogic)

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

1. "Installing Tivoli Storage Manager client"  
Install the Tivoli Storage Manager client software on each application server where Content Engine is deployed.
2. "Copying the Tivoli Storage Manager API library files to additional servers"  
If you are running a Content Engine server farm, the Tivoli Storage Manager API libraries must be on each server in the farm.
3. "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.

#### Installing Tivoli Storage Manager client:

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

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 fixed content device in FileNet Enterprise Manager. If you are installing Tivoli Storage Manager client on multiple UNIX hosts, the installation path must be the same on each host. On AIX, install Tivoli Storage Manager client at `/usr/tivoli/tsm/client/ba/bin`.

#### Copying the Tivoli Storage Manager API library files to additional servers:

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

Copy the entire tsm100directory structure from the Content 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
UNIX	/opt/FileNet/ContentEngine/tsm100
Windows	C:\Program Files\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.

1. Open in an edit window the WebLogic script that sets up the domain environment. The following are example paths to this script:

Option	Description
UNIX	/opt/bea/user_projects/domains/ base_domain/bin/setDomainEnv.sh
Windows	C:\bea\user_projects\domains\ base_domain\bin\setDomainEnv.cmd

2. Edit the WebLogic script by adding the lines shown below, for your operating system, just before the line in which the WL\_HOME variable is set. Substitute your version identifier in place of weblogic92 as appropriate. There is no carriage return after any line that ends with /, \, : or \_.

Option	Description
AIX	TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 LIBPATH=\${LIBPATH}:\${TSMAPILIB} EXT_POST_CLASSPATH= \${EXT_POST_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export LIBPATH EXT_POST_CLASSPATH WL_HOME="/opt/bea/weblogic92" export WL_HOME
HP-UX (32-bit)	TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 SHLIB_PATH=\${SHLIB_PATH}:\${TSMAPILIB} EXT_POST_CLASSPATH= \${EXT_POST_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export SHLIB_PATH EXT_POST_CLASSPATH WL_HOME="/opt/bea/weblogic92" export WL_HOME
HP-UX (64-bit) and HP-UXi	TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 SHLIB_PATH=\${SHLIB_PATH}:\${TSMAPILIB} EXT_POST_CLASSPATH= \${EXT_POST_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export SHLIB_PATH EXT_POST_CLASSPATH JAVA_OPTIONS="\${JAVA_OPTIONS} -d64" export JAVA_OPTIONS WL_HOME="/opt/bea/weblogic92" export WL_HOME
Linux	TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 LD_LIBRARY_PATH=\${LD_LIBRARY_PATH}: \${TSMAPILIB} EXT_POST_CLASSPATH= \${EXT_POST_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export LD_LIBRARY_PATH EXT_POST_CLASSPATH WL_HOME="/opt/bea/weblogic92" export WL_HOME



Option	Description
Solaris (32-bit)	TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 TSMCLIENTLIB=/opt/tivoli/tsm/ client/api/bin LD_LIBRARY_PATH=\${LD_LIBRARY_PATH}: \${TSMAPILIB}:\${TSMCLIENTLIB} EXT_POST_CLASSPATH= \${EXT_POST_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export LD_LIBRARY_PATH EXT_POST_CLASSPATH WL_HOME="/opt/bea/weblogic92" export WL_HOME
Solaris (64-bit)	TSMCLIENTLIB=/opt/tivoli/tsm/ client/api/bin64 LD_LIBRARY_PATH_64= \${LD_LIBRARY_PATH_64}: \${TSMAPILIB}:\${TSMCLIENTLIB} EXT_POST_CLASSPATH= \${EXT_POST_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export LD_LIBRARY_PATH_64 EXT_POST_ CLASSPATH JAVA_OPTIONS="\${JAVA_OPTIONS} -d64" export JAVA_OPTIONS WL_HOME="/opt/bea/weblogic92" export WL_HOME
Windows	set TSMAPILIB=C:\Program Files\IBM\ FileNet\ContentEngine\tsm100 set PATH=%PATH%;%TSMAPILIB% set EXT_POST_CLASSPATH=%EXT_POST_ CLASSPATH%;%TSMAPILIB%\TsmJavaApi.jar set WL_HOME=C:\bea\weblogic92

3. If you are using WebLogic Node Manager to start and stop WebLogic Managed Servers in a clustered environment, you must enable Node Manager to use the appropriate start script:
  - a. Open for editing the node manager configuration file WL\_HOME/common/nodemanager/nodemanager.properties.
  - b. Set the StartScriptEnabled property to true (default is false).
  - c. Set the StartScriptName to match the script name used by Node Manager to start the managed server, depending on your operating system:

Option	Description
UNIX	StartScriptName=startManagedWebLogic.sh
Windows	StartScriptName=startManagedWebLogic.cmd

**Important:** If the managed server is not on the same machine as the WebLogic Administration Server and you have an alternate script matching the name of the Managed Server in the domain bin directory, make sure to specify that script name instead of the more generic "startManagedWebLogic" script.

4. Save your edits in nodemanager.properties and restart the Node Manager.

## Installing Tivoli Storage Manager client and adding native API library paths (JBoss)

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

1. "Installing Tivoli Storage Manager client"  
Install the Tivoli Storage Manager client software on each application server where Content Engine is deployed.
2. "Copying the Tivoli Storage Manager API libraries to additional servers"  
If you are running a Content Engine server farm, the Tivoli Storage Manager API libraries must be on each server in the farm.
3. "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.

### Installing Tivoli Storage Manager client:

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

1. Download the Tivoli Storage Manager client software from the IBM Support site at <http://www-01.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 will need to specify the path as the DSMI directory when you create a Tivoli fixed content device in FileNet Enterprise Manager. If you are installing Tivoli Storage Manager client on multiple UNIX hosts, the installation path must be the same on each host. On AIX, install Tivoli Storage Manager client at `/usr/tivoli/tsm/client/ba/bin`.

### Copying the Tivoli Storage Manager API libraries to additional servers:

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

Copy the entire `tsm100` directory structure from the Content 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
UNIX	<code>/opt/IBM/FileNet/ContentEngine/tsm100</code>
Windows	<code>C:\Program Files\IBM\FileNet\ContentEngine\tsm100</code>

### 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.

1. Open in an edit window the JBoss startup script that sets up the domain environment:

Option	Description
UNIX	<code>run.sh</code>

Option	Description
Windows	run.bat

- Edit the startup script by adding the following lines at the start of the script. There is no carriage return after any line that ends with /, \, : or \_.

Option	Description
AIX	TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 LIBPATH=\${LIBPATH}:\${TSMAPILIB} JBOSS_CLASSPATH=\${JBOSS_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export LIBPATH JBOSS_CLASSPATH
HP-UX (32-bit)	TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 TSMCLIENTLIB=/opt/tivoli/tsm/client/api/ bin64 SHLIB_PATH=\${SHLIB_PATH}:\${TSMAPILIB}: \${TSMCLIENTLIB} JBOSS_CLASSPATH=\${JBOSS_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export SHLIB_PATH JBOSS_CLASSPATH
HP-UX (64-bit) and HP-UXi	TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 TSMCLIENTLIB=/opt/tivoli/tsm/client/api/ bin64 SHLIB_PATH=\${SHLIB_PATH}:\${TSMAPILIB}: \${TSMCLIENTLIB} JBOSS_CLASSPATH=\${JBOSS_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export SHLIB_PATH JBOSS_CLASSPATH JAVA_OPTS="\${JAVA_OPTS} -d64" export JAVA_OPTS
Linux	TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 LD_LIBRARY_PATH=\${LD_LIBRARY_PATH}: \${TSMAPILIB} JBOSS_CLASSPATH=\${JBOSS_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export LD_LIBRARY_PATH JBOSS_CLASSPATH
Solaris (32-bit)	TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 TSMCLIENTLIB=/opt/tivoli/tsm/client/api/ bin LD_LIBRARY_PATH=\${LD_LIBRARY_PATH}: \${TSMAPILIB}:\${TSMCLIENTLIB} JBOSS_CLASSPATH=\${JBOSS_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export LD_LIBRARY_PATH JBOSS_CLASSPATH
Solaris (64-bit)	TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 TSMCLIENTLIB=/opt/tivoli/tsm/client/api/ bin64 LD_LIBRARY_PATH_64=\${LD _LIBRARY_PATH_64}:\${TSMAPILIB}: \${TSMCLIENTLIB} JBOSS_CLASSPATH=\${JBOSS_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export LD_LIBRARY_PATH_64 JBOSS _CLASSPATHJAVA_OPTS="\${JAVA_OPTS} -d64" export JAVA_OPTS

Option	Description
Windows	<pre>set TSMAPILIB=C:\Program Files\IBM\ FileNet\ContentEngine\tsm100 set PATH=%PATH%;%TSMAPILIB% set JBOSS_CLASSPATH=%JBOSS_ CLASSPATH%;%TSMAPILIB%\TsmJavaApi.jar</pre>

## Installing or updating EMC Centera SDK library files

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

Update the EMC Centera SDK library files if Centera fixed content devices are in your existing environment or if Centera fixed content devices will be added to your IBM FileNet P8 environment.

1. "Installing EMC Centera SDK version 3.2 library files"  
EMC Center SDK library files enable access between the IBM FileNet P8 environment and EMC Centera fixed content devices.
2. "Configuring EMC Centera SDK environment variables for version 3.2" on page 270  
Specify values for the environment variables so that Content Engine can access the EMC Centera SDK library files.

### Installing EMC Centera SDK version 3.2 library files:

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

1. Log on to the Content Engine Server machine as *ce\_install\_user*.
2. Back up or delete any existing EMC Centera SDK library files, which are located in the Default Destination Installation Location column of the following table:

Operating System	Default Destination Installation Location
AIX	/usr/local/Centera_SDK
Solaris	/opt/Centera_SDK
Windows	C:\Centera_SDK
Linux	/usr/local/Centera_SDK
HP-UX	/opt/Centera_SDK
HP-UXi	/opt/Centera_SDK

3. The Centera directory in the Content Engine software package contains the Centera SDK version 3.2 installation files. As shown in the following table, copy the appropriate directory to a location on the Content Engine Server machine, such as /tmp (UNIX) or C:\Temp (Windows).

Operating System	Directory To Be Copied
AIX, Solaris, Windows	Copy the entire Centera directory
Linux	Depending on your version of gcc, copy one of the following directories: Centera/gcc3.3 Centera/gcc4
HP-UX 11i v1 (11.11)	Copy Centera/11i-v1-11.11

Operating System	Directory To Be Copied
HP-UX 11i v2 (11.23)	Copy Centera/11iv1-11.23

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

Option	Description
UNIX	<code>install.sh</code>
Windows	<code>install.bat C:\Centera_SDK</code>

- The installer script creates both 32-bit and 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.

Operating System	Subdirectories of extracted EMC Centera SDK Directory	Description
AIX, Solaris, and Windows	<code>lib</code>	<code>lib</code> has the native library files that are to be installed.
Linux	<code>../gcc3.3/lib</code>	
	<code>../gcc4/lib</code>	
HP-UX	<code>../11i-v1-11.11/lib</code>	
HP-UXi	<code>../11i-v1-11.13/lib</code>	

### Configuring EMC Centera SDK environment variables for version 3.2:

Specify values for the environment variables so that Content Engine can access the EMC Centera SDK library files.

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

Option	Description
UNIX	<code>setCenteraLibPath.sh</code>
Windows	<code>setCenteraLibPath.bat</code>

- Modify the sample setup script as indicated in the following table:

Note that the `CENTERA_LIB_PATH` variable needs to point to the sample script, not just the installation directory that contains the script.

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/SDK3.2.607`

then change the installation path of the AIX script to:

/usr/local/Centera/SDK3.2.607/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.

Operating System	Script Revisions
AIX	<p>From:</p> <pre>CENTERA_LIB_PATH=/usr/local/Centera_SDK/lib/32 LIBPATH=\$LIBPATH:\$CENTERA_LIB_PATH export LIBPATH</pre> <p>to:</p> <pre>CENTERA_LIB_PATH= install_path /lib/32</pre> <p>or:</p> <pre>CENTERA_LIB_PATH= install_path /lib/64</pre>
Solaris	<p>From:</p> <pre>CENTERA_LIB_PATH=/opt/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>
Linux	<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>

Operating System	Script Revisions
HP-UX HP-UXi	<p>From:</p> <pre>CENTERA_LIB_PATH=/opt/Centera_SDK/lib/32 SHLIB_PATH=\$SHLIB_PATH:\$CENTERA_LIB_PATH export SHLIB_PATH</pre> <p>to:</p> <pre>CENTERA_LIB_PATH=<i>install_path</i>/lib/32 SHLIB_PATH=\$SHLIB_PATH:\$CENTERA_LIB_PATH export SHLIB_PATH</pre> <p>or:</p> <pre>CENTERA_LIB_PATH=<i>install_path</i>/lib/64 SHLIB_PATH=\$SHLIB_PATH:\$CENTERA_LIB_PATH export SHLIB_PATH</pre>
Windows	<p>From:</p> <pre>set CENTERA_LIB_PATH=C:\Centera_SDK\lib\32 set PATH=%PATH%;%CENTERA_LIB_PATH%</pre> <p>to:</p> <pre>set CENTERA_LIB_PATH=<i>install_path</i> \lib\32 set PATH=%PATH%;%CENTERA_LIB_PATH%</pre> <p>or:</p> <pre>set CENTERA_LIB_PATH=<i>install_path</i> \lib\64 set PATH=%PATH%;%CENTERA_LIB_PATH%</pre>

- 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.

Application Server	Startup Script (UNIX)	Startup Script (Windows)
WebSphere	setupCmdLine.sh	setupCmdLine.cmd
WebLogic	setDomainEnv.sh	setDomainEnv.cmd
JBoss	run.sh	run.cmd

- Stop and start the application server.

## Completing Content Engine post-deployment steps

You must complete several Content Engine post-deployment steps before you can put an IBM FileNet P8 system into production.

Perform the post-deployment procedures for your application server type, and then perform the Content Engine verification procedures.

- “Completing post-deployment steps (WebSphere Application Server)” on page 273  
If you are using IBM WebSphere Application Server federated user repositories, you must specify the primary administrative user for the web application server.
- “Completing post-deployment steps (Oracle WebLogic Server)” on page 273  
You must restart the web application server to reinitialize the server cache.
- “Completing post-deployment steps (JBoss Application Server and Active Directory)” on page 273



You must edit the <login-module> XML element in the login-config.xml file to complete the authentication configuration for the Content Engine application.

4. “Verifying the Content Engine deployment” on page 274  
You can verify that the Content Engine deployment was successful by accessing the IBM FileNet P8 System Health page.

### Completing post-deployment steps (WebSphere Application Server)

If you are using IBM WebSphere Application Server federated user repositories, you must specify the primary administrative user for the web application server.

To set the administrative user

1. Log in to the WebSphere administrative console.
2. Navigate to **Security** → **Secure administration, applications, and infrastructure**, and click **Configure**.
3. If you have not already done so, specify a unique user (short name) for the **Primary administrative user name**.

**Important:** This name must exist in one of the realms and must be unique.

4. Specify the **Server user identity**. You can specify **Automatically generated server identity**, or specify a user name that exists in one of the repositories. This name must exist in one of the realms and must be unique.
5. Save your changes to the master configuration.
6. If you are upgrading from version 3.5, enable administrative security and application security. The deployment of Content Engine does not enable or check these settings.

**Important:** You must disable Java2 security; otherwise, Content Engine will not be able to start or process requests.

7. Restart the web application server where Content Engine is deployed, as follows:
  - For a stand-alone server, stop and start the application server.
  - For a network deployment on WebSphere Application Server Network Deployment, stop and start the application server where Content Engine is deployed, including the Deployment Manager and all managed nodes.
  - For a cluster, stop and start the cluster.

### Completing post-deployment steps (Oracle WebLogic Server)

You must restart the web application server to reinitialize the server cache.

Restart the Oracle WebLogic Server where Content Engine is deployed.

- For a stand-alone server, stop and start the application server.
- For a cluster, stop and start the cluster.

### Completing post-deployment steps (JBoss Application Server and Active Directory)

You must edit the <login-module> XML element in the login-config.xml file to complete the authentication configuration for the Content Engine application.

1. Make a backup of the file JBOSS\_HOME/server/CE\_server\_path/conf/login-config.xml, where ce\_server\_path is, for example, default.
2. Open the login-config.xml file for editing.

3. Locate the following line inside the scope of the <login-module> XML element at the beginning of the file:

```
<login-module code="org.jboss.security.auth.spi.LdapExtLoginModule"
 flag="required">
```

Edit the line as follows:

```
<login-module code="org.jboss.security.auth.spi.LdapExtLoginModule"
 flag="sufficient">
```

4. Add the following line immediately after the <login-module line:
 

```
<module-option name="java.naming.referral">follow</module-option>
```
5. Save your changes.
6. Start the JBoss web application server.

## Verifying the Content Engine deployment

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

1. Verify the state of Content Engine deployment by browsing to the IBM FileNet P8 System Health page:

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

where:

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

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

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

Table 26. Example FileNet P8 System Health page address

Application Server Type	Web Page Address
IBM WebSphere Application Server	<code>http://server:9080/P8CE/Health</code>
Oracle WebLogic Server	<code>http://server:7001/P8CE/Health</code>
JBoss Application Server	<code>http://server:8080/P8CE/Health</code>

2. Verify that the FileNet P8 System Health page contains the Content 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. In particular, if you are upgrading from version 3.5.2, a red icon appears before the GCD, directory configurations, object stores, storage areas, and sites entries. Also, if you are upgrading from version 3.5.2, no domain name appears yet in the Domain entry.

Table 27. FileNet P8 System Health page contents

Section	Description
<b>Domain</b>	Displays the FileNet P8 domain name if a domain was found.
<b>Global Configuration Database</b>	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.
<b>Directory Configurations</b>	Verifies that at least one directory service is configured and lists the number of configured directory service providers.

Table 27. FileNet P8 System Health page contents (continued)

Section	Description
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 FileNet Engine Web page:  
`http://server:port/FileNet/Engine`  
 where:  
*server* is the host name of the machine where Content Engine is deployed.  
*port* is the HTTP port used by the application server where Content Engine is deployed.  
 The following table lists an example address for your application server:

Table 28. Example FileNet Engine Web page address

Application Server Type	Web Page Address
IBM WebSphere Application Server	<code>http://myserver:9080/FileNet/Engine</code>
Oracle WebLogic Server	<code>http://myserver:7001/FileNet/Engine</code>
JBoss Application Server	<code>http://myserver:8080/FileNet/Engine</code>

5. Verify that the FileNet Engine Web page contains the following information:
  - Verify the value in the **Startup Message** key. The Content Engine build and version (for example, dap451.097), 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 Engine software is installed.
  - Verify the value in the **Process Engine** key. The Process Engine Client build and version (for example, pui451.075), must match the build and version in the *version.txt* file in the TAR or ZIP file of the Process Engine Client installation software.
  - Verify that the values for JDBC driver, server instance, operating system, and other properties match the values that you entered when you configured Content Engine.
6. Optional: Bookmark the FileNet Engine Web page in your browser for later use.

## Installing the latest Content Engine client files on other IBM FileNet P8 servers (for staged upgrades)

When you upgrade Content Engine software, you must also upgrade the associated Content Engine Client files installed on other machines running IBM FileNet P8 components, for example, on Process Engine and Application Engine servers.

In a standard upgrade of your IBM FileNet P8 system, you would install these client files in the course of upgrading each respective component.

However, if you are staging your IBM FileNet P8 upgrade over a period of time and not upgrading one or more of the other IBM FileNet P8 components at this time, you must still perform the Content Engine Client install on the other component machines. In this case, use the following topics in the sections for the other components:

- “Upgrading the Content Engine client files on Process Engine servers” on page 416
- “Installing the latest Content Engine client files on Application Engine servers” on page 449

### **Important:**

- You must install the Content Engine client files for any expansion products that use Content Engine Client files, such as:
  - IBM FileNet Workplace XT
  - IBM InfoSphere Enterprise Records
  - IBM FileNet Business Process Framework
- You must redeploy any components that are web-application-server-based, such as Application Engine, Workplace XT, and InfoSphere Enterprise Records, after you upgrade the Content Engine Client files on the associated machines.

## Establishing the FileNet P8 domain and Global Configuration Data

You must use IBM FileNet Enterprise Manager to create a FileNet P8 domain and the Global Configuration Data (GCD).

Complete the procedures for the FileNet P8 domain and the Global Configuration Data (GCD).

1. “Creating the FileNet P8 domain”  
You use IBM FileNet Enterprise Manager to create the FileNet P8 domain.
2. “Configuring directory service authentication” on page 277  
You must configure the directory service authentication for the domain. To set up multi-realm authorization, you must run the Create a Directory Configuration wizard one time for each realm.
3. “Configuring permissions for a FileNet P8 domain” on page 278  
You must configure the permissions for the FileNet P8 domain. To complete this configuration, you add your authorized users and groups to the list of Global Configuration Data (GCD) administrators.
4. “Verifying the trace log file location” on page 278  
You must verify that trace log file location after you deploy Content Engine.

### **Creating the FileNet P8 domain**

You use IBM FileNet Enterprise Manager to create the FileNet P8 domain.

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

**Important:** If you run Enterprise Manager as a limited user account, you cannot update the Base URL for the FileNet P8 Platform help files field in the General tab of the Enterprise Manager properties dialog box.


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. To view only Content Engine values for this task, filter by **EM: Create FileNet P8 domain** in the **Installation or Configuration Program** column.

2. Start Enterprise Manager by double-clicking the **Enterprise Manager** icon on the desktop, or by choosing **Start → All Programs → FileNet P8 Platform → Enterprise Manager**.
3. Click **Add** and complete the configuration screens by using the values in your worksheet. The initial values displayed in the screens are default values that you must change to match your site.

#### 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 directory service authentication

You must configure the directory service authentication for the domain. To set up multi-realm authorization, you must run the Create a Directory Configuration wizard one time for each realm.

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

See these FileNet P8 help topics for additional information:

- **System Administration → Enterprise-wide Administration → FileNet P8 Security → How to → Configure for multiple realms**
- **System Administration → Enterprise-wide Administration → FileNet P8 Security → Directory service providers.**

To configure directory service authentication:

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 for this task, filter by **EM: Create a Directory Configuration** in the **Installation or Configuration Program** column.


2. In the FileNet P8 dialog box, click **Connect**.
3. In the Create P8 Domain screen, enter the name for a new FileNet P8 domain and click **Continue** to start the Create a Directory Configuration wizard.

If an error occurs, check the application server log file on the machine where Content Engine is deployed:

Application server type	Path to log file
IBM WebSphere Application Server	<i>WAS_install_path</i> /AppServer/profiles/ <i>profile_name</i> /logs/server_name/SystemOut.log
Oracle WebLogic Server	<i>WLS_install_path</i> /user_projects/domains/ <i>domain_name</i> /servers/server_name/logs/server_name.log
JBoss Application Server	JBOSS_DIST/server/server_name/log/server_name.log

- Complete the configuration screens by using the values in your worksheet.
- In the Configure New Domain Permissions message box, click **OK** to acknowledge that the directory configuration is complete but remains in restricted mode. The Configure New Domain Permissions wizard automatically starts if you are using Enterprise Manager for the first time and have not defined any Global Configuration Data (GCD) administrators.

#### 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 permissions for a FileNet P8 domain

You must configure the permissions for the FileNet P8 domain. To complete this configuration, you add your authorized users and groups to the list of Global Configuration Data (GCD) administrators.

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


To configure permissions for a FileNet P8 domain:

- 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 **EM: Configure New Domain Permissions** in the **Installation or Configuration Program** column.

- Complete the configuration screens by using the values in your worksheet.
- In the Configure New Domain Permissions message box, click **OK**.

#### 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*.

### Verifying the trace log file location

You must verify that trace log file location after you deploy Content Engine.

Perform the following steps to check the path to the trace log file, *p8\_server\_trace.log*.

- Start IBM FileNet Enterprise Manager by double-clicking the **Enterprise Manager** icon on the desktop, or by choosing **Start** → **All Programs** → **FileNet P8 Platform** → **Enterprise Manager**.

2. Navigate to the level (domain, site, virtual server, or server instance) at which trace logging is configured, right-click the node at that level, and choose **Properties**.
3. Click the **Trace Control** tab.
4. If the current value of the **Log File Output Location** parameter is not consistent with the version of the application server, then edit the value as needed.

The following table shows default locations, at the server instance level, for the trace log file, starting at *install\_root*, the installation path for the application server.

Application Server Type	Path to Trace Log File
IBM WebSphere Application Server	<i>install_root</i> /profiles/ <i>profile_name</i> / FileNet/ <i>server_name</i> / p8_server_trace.log
Oracle WebLogic Server	<i>install_root</i> /user_projects/domains/ <i>domain_name</i> /FileNet/ <i>server_name</i> / p8_server_trace.log
JBoss Application Server	<i>install_root</i> /bin/FileNet/ <i>server_name</i> / p8_server_trace.log

5. Click **OK**.

## Configuring storage devices for upgrades

When you upgrade from Content Engine version 3.5.2, you must configure your existing file store devices.

Complete the procedure for the devices in your environment.

“Configuring storage devices for migration to UNIX”

When you upgrade from Content Engine version 3.5.2 and migrate to a UNIX server, you must prepare the UNIX server to mount your existing file store devices.

“Preparing NetApp SnapLock volumes for upgrade” on page 280

If your existing IBM FileNet P8 domain includes a SnapLock fixed content device, you must allow access to your fixed content via NFS instead of, or in addition to, CIFS.

## Configuring storage devices for migration to UNIX

When you upgrade from Content Engine version 3.5.2 and migrate to a UNIX server, you must prepare the UNIX server to mount your existing file store devices.

To prepare file store devices when migrating to UNIX:

Install and configure your choice of software to permit the Content Engine UNIX server to mount your existing version 3.5.2 file store devices.

- If you are migrating your Content Engine version 3.5.2 file storage devices to UNIX, you must copy your existing storage directories and files to the UNIX machine and ensure that the *ce\_os\_user* account has permissions for the new directories and folders.
- If the version 3.5.2 file storage areas remain on the Windows NTFS devices, or if you intend to use the Content Engine Upgrader tool rather than Content Engine Web Upgrade Tool to upgrade your object stores (regardless of whether you leave the storage directories on NTFS or the UNIX file system), create an NFS mount from the Content Engine version 4.5.1 server to the NTFS mount.



## Related tasks

“Installing or upgrading Content Engine” on page 225

You can install or upgrade Content Engine, Configuration Manager, .NET Clients (including IBM FileNet Enterprise Manager), Content Engine Upgrader, and FileNet Deployment Manager either interactively or silently.

## Preparing NetApp SnapLock volumes for upgrade

If your existing IBM FileNet P8 domain includes a SnapLock fixed content device, you must allow access to your fixed content via NFS instead of, or in addition to, CIFS.

1. Check the prerequisites.
  - a. Check the *IBM FileNet P8 Hardware and Software Requirements* to verify your NetApp filers use the version of the Data ONTAP operating system that is supported in version 4.5.1 of IBM FileNet P8.  
For information on accessing and configuring your NetApp filers, consult the following Data ONTAP manuals:
    - *System Administration Guide*
    - *Software Setup Guide*
    - *File Access and Protocols Management Guide*
  - b. Make sure you are licensed to use NFS to access your NetApp filers.
2. Set the security style of a NetApp storage volume to enable support for NFS clients.

Each qtree (virtual subvolume of a storage volume) has exactly one of the security styles (scheme for setting security on files and directories in the qtree) shown in the following table:

Security Style	Description
UNIX	UNIX file permission attributes. Only NFS clients can create files and directories in a UNIX qtree.
NTFS	Windows access control lists. Only CIFS clients can create files and directories in an NTFS qtree.
Mixed	Both UNIX and NTFS security styles. Only one security style at a time is allowed. The current style is that of the last client to modify it.

Because all pre-4.0.0 versions of IBM FileNet P8 support only CIFS, all NetApp storage volumes used by Content Engine version 3.5.2 use NTFS security style. You must change the security style to UNIX or Mixed. Specify the Mixed style for qtrees that must service requests for both NFS and CIFS clients during the upgrade process; otherwise, specify UNIX style.

For each qtree, perform the following steps to specify the security style:

- a. Access the Data ONTAP administrative console. See the ONTAP System Administration Guide for information on administrative access methods.
- b. Run the qtree command as in the following example, which sets the UNIX security style on the qtree `/vol/vol1/sa1` of NetApp filer `NAFiler` to UNIX:

```
telnet NAFiler
qtree security /vol/vol1/sa1 unix
```

After the qtree command executes, all files created by Content Engine on a UNIX platform will have UNIX security attributes.

3. Map UNIX users and groups to Window equivalents.

Because Content Engine version 3.5.2 support CIFS, rather than NFS, all existing files on a NetApp volume have NTFS security attributes. The users and groups with access rights to these files are defined by Windows.

To allow the version 3.5.2 files to remain accessible, you must create a mapping between the new UNIX account for version 4.5.1 of Content Engine and the old Windows account for version 3.5.2.

Each NetApp filer has its own configuration file, `/etc/usermap.cfg`, to map between Windows user names and equivalent UNIX user names. A UNIX user attempting to access a file having NTFS security attributes uses `usermap.cfg` to determine if a mapping exists between the UNIX account and an equivalent Windows account. If the mapping exists, the access checks on the target file will use the Windows account.

Each `usermap.cfg` entry has the following format:

`[ IP_qualifier :] Windows_name [ direction ] [ IP_qualifier :] UNIX_name`

The meaning of each element in the entry is shown in the following table:

Element	Meaning
<i>IP_qualifier</i>	Qualifies the name according to the source address of the requester
<i>Windows_name</i>	The name of the Window user or group in domain name format (for example, <i>DomainName\UserName</i> ). The Windows name must be in the Windows domain that the NetApp filer is configured to use when authenticating Windows users.
<i>UNIX_name</i>	The name of a UNIX user or group. The name must be defined in the file or directory service that the NetApp filer uses to authenticate UNIX users. In many cases this will be the local <code>/etc/passwd</code> (for users) or <code>/etc/group</code> (for groups).  If it is a group, it might be necessary to also define it in an NIS repository or an LDAP directory server, depending on how the filer is configured.  In either case the UID (UNIX user ID) must be identical to the UID of the user under which the Content Engine Server is executing.
<i>Direction</i>	The direction of the mapping, either <code>&lt;=</code> or <code>=&gt;</code> .  <code>&lt;=</code> : Maps <i>UNIX_name</i> to <i>Windows_name</i> <code>=&gt;</code> : Maps <i>Windows_name</i> to <i>UNIX_name</i>

For example, the following steps define a mapping on a NetApp filer between FNCE\_OS\_User (the Windows user account under which version 3.5.2. *x* of Content Engine Server executes) and FNCE\_UNIX\_User (the UNIX user account under which version 4.5.1 of Content Engine Server executes).

- a. Log on to the machine where version 3.5.2 of the Content Engine is installed.

- b. Connect to the root volume on the target NetApp filer by using the Administrator account.

By default, the NetApp filer root volume is accessible from a Windows client as a CIFS share named C\$, as in the following example (where *NAFiler* is the host name of the target NetApp filer at your site).

```
C\> net use n: \\NAFiler\C$ /user:NAFiler1\Administrator
```

- c. Edit `/etc/usermap.cfg` by adding the following stanza:

```
CEDomain\FNCE_OS_User => FNCE_UNIX_User
```

- d. Edit `/etc/passwd` by adding the following stanza:

```
FNCE_UNIX_User:CEServers:205:7100:~/home/FNCE_UNIX_User:
```

4. Return to the parent topic and complete the task.

#### Related information

 Product documentation for IBM FileNet P8 Platform  
Download the IBM FileNet P8 Hardware and Software Requirements, as well as PDF's of the rest of the IBM FileNet P8 Platform documentation.

## Creating the data sources for an object store

Each object store in your site requires its own JDBC data sources. You can configure the data sources by using the Configuration Manager graphical user interface or the command line.

You created the JDBC data source for the Global Configuration Data (GCD) earlier in the configuration process. You must add the data sources now for at least one object store that you want to upgrade. You can create additional object store data sources as needed either immediately after you create the initial object store data sources or after you have confirmed your Content Engine configuration.

**Restriction:** Configuration Manager cannot create a data source that uses the same name as an existing data source. If you manually configured a data source by using your web application server administration tools, and you want to reuse the name, then you must manually delete the existing data source before you attempt to create the data source in Configuration Manager. See your web application server documentation for more information.

“Creating the initial object store data sources by using the graphical user interface” on page 283

You must create the JDBC data sources for each object store that Content Engine uses. Content 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 a single object store.

“Creating additional object store data sources by using the graphical user interface” on page 283

You must create the JDBC data sources for each object store that Content Engine uses. Content 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 a single object store, and you can add additional tasks as needed for each additional object store.

“Creating the data sources by using the command line” on page 285

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

## Creating the initial object store data sources by using the graphical user interface

You must create the JDBC data sources for each object store that Content Engine uses. Content 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 a single object store.

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 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 29. Required application server state

Option	Description
WebSphere Application Server	Start the application server if it is not already running.
JBoss Application Server	Stop the application server.
Oracle WebLogic Server	Start the application server 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. Select **File** → **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 the task is enabled. 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 context 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 task execution status messages are displayed in the Console pane below the bootstrap properties.
10. (JBoss only) Start the application server.

## Creating additional object store data sources by using the graphical user interface

You must create the JDBC data sources for each object store that Content Engine uses. Content 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 a single object store, and you can add additional tasks as needed for each additional object store.

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

The default configuration profile contains one task for configuring a single object store. You must create and run a new task for each additional object store in that Content Engine uses.

To configure the JDBC settings for additional object stores:

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 **CM: Configure JDBC data sources (object store 2)** in the **Installation or Configuration Program** column.

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

Table 30. Required application server state

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

3. If your configuration profile is not open in Configuration Manager, open it by select **File → Open** and navigating to your *profilename.cfgp* file.
4. Create a task for the additional object store.
  - a. Right-click any *task name* in the profile pane, such as **Configure Object Store JDBC Data Sources**, and select **Add New Task → Configure JDBC Data Sources**. The **New\_Configure JDBC Data Sources** task is added to the profile.
  - b. Right-click **New\_Configure JDBC Data Sources**, and select **Rename Task**.
  - c. Enter a useful name for the task, such as **Configure Object Store 2 JDBC Data Sources**.
  - d. Click **OK**.
5. Right-click the **Configure Object Store 2 JDBC Data Sources** task in the profile pane, and select **Edit Selected Task**.
6. Provide the property values for the JDBC data sources for the object store by using the values in your worksheet for your additional object store.
7. Select **File → Save** to save your changes.
8. 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.
9. Ensure that the task is enabled. When the task is disabled, the task name includes the text **(disabled)**. To enable the task, right-click **Configure Object Store 2 JDBC Data Sources (disabled)** in the profile pane, and choose **Enable Selected Task** from the context menu.
10. Apply the JDBC property settings by right-clicking **Configure Object Store 2 JDBC Data Sources** 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.

11. (JBoss only) Start the application server.
12. Optional: Repeat this procedure as needed to add the data sources for each object store in your environment.

### Creating the data sources by using the command line

You must create the JDBC data sources for each object store that Content Engine uses. You must generate, edit, and execute a new `configurejdbc-os.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 `configurejdbc-os.xml` file for the initial object store data sources. If you have an existing `configurejdbc-os.xml` file, you can generate another file for each additional object store. Each additional file that you add is named `configurejdbc-os.n.xml`. You can generate multiple `configurejdbc-os.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 `configurejdbc-os.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 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 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 `configurejdbc-os.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 ConfigureJDBC -profile myprofile
```
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 3 on page 285 through 6 as needed for each additional object store.

## Upgrading Content Search Engine software from version 3.5.2

If you used the full-text search feature (CBR) in version 3.5.2, you upgrade by installing and configuring version 4.5.1 of Content Search Engine (Autonomy K2). After the upgrade, you recreate index areas, called *K2 collections*, to replace the version 3.5.2 content search indexes.

**Important:** If version 4.5.1 of Content Search Engine is already part of your existing version 4.5.1 Content Engine system, omit the tasks in this section.

As of the 4.0 release of P8 Platform, the full-text search feature was removed as a built-in function of the Content Engine. Instead, the remote Autonomy K2 Content Search Engine software is installed and configured through Enterprise Manager to enable full-text searching.

To upgrade Content Search Engine from version 3.5.2 to 4.5.1, you can install and configure the Autonomy K2 product before or after you upgrade Content Engine. After upgrading Content Search Engine, you create new index areas, and specify classes and property templates for those classes (if so desired). Then you run a classes index job, which is part of the upgrade of Content Engine.

1. "Production environment upgrades" on page 287  
Upgrade of Content Search Engine and related Content Engine data must occur



as an in-place upgrade. As such, the data is migrated to version 4.5.1 and is no longer usable in the previous version of IBM FileNet P8.

2. "Content Search Engine software upgrade"  
The Autonomy K2 software must be installed on each machine that is part of your Content Search Engine configuration. You must designate one machine in the configuration as the Master Administration Server.
3. "Upgrading Content Search Engine (UNIX)" on page 288  
You must install the K2 Master Administration Server software first. The Master Administration Server dashboard is the central control point for configuring Content Search Engine for single-server or multiserver installations.
4. "Upgrading Content Search Engine (Windows)" on page 292  
Install and configure IBM FileNet P8 Content Search Engine,
5. "Updating the style file of user fields" on page 294  
You need to edit the Autonomy K2 style file of user fields to add a data field definition for storing the partitioning value of a document.
6. "Configuring Content Search Engine" on page 294  
You can configure services required on the K2 Master Administration Server, and on additional Administration Servers you might install for IBM FileNet P8 Content Search Engine. All servers are configured through the Master Administration Server Dashboard.
7. "Configuring Autonomy K2 for version 4.5.1 index areas" on page 299  
For performance reasons, it is recommended that you create one collections directory for each index area you create in IBM FileNet P8 Content Engine. Each collections directory you create must be set to provide proper security access. The path to both the collections directory and collections temp directory must be entered in the index area properties when you create them.

## **Production environment upgrades**

Upgrade of Content Search Engine and related Content Engine data must occur as an in-place upgrade. As such, the data is migrated to version 4.5.1 and is no longer usable in the previous version of IBM FileNet P8.

To perform an upgrade in a migration scenario, create a duplicate of your FileNet P8 system by performing a backup and then a restore. Using the restored system, complete the migration from version 3.5.2 to 4.5.1. This will leave the original production environment untouched while testing is performed on the new system.

When you're ready to migrate the production environment to the current version, back up the system and then perform the in-place upgrade on the production environment.

## **Content Search Engine software upgrade**

The Autonomy K2 software must be installed on each machine that is part of your Content Search Engine configuration. You must designate one machine in the configuration as the Master Administration Server.

The Master Administration Server can be used as a stand-alone Content Search Engine, or additional K2 Administration Servers can be added. All K2 Administration servers are configured and controlled through the K2 Dashboard of the Master Administration server.

The Autonomy K2 software that underlies IBM FileNet P8 Content Search Engine has many inherent features that you might want to configure that are not discussed in the IBM FileNet documentation. For details, see the Autonomy

documentation that is installed with the Autonomy K2 Master Administration Server located at: [http://Master Administration Server hostname:9990/verity\\_docs/](http://Master Administration Server hostname:9990/verity_docs/)

The Autonomy documentation set is not searchable from the IBM FileNet P8 Help but it does have its own internal index and search functionality.

**Important:** Although the K2 Dashboard provides you with documentation for, and direct interfaces to, the K2 collections, IBM FileNet requires that you use Enterprise Manager to manage collections associated with Content Search Engine index areas (for example, to add and remove index areas).

- Autonomy K2 was previously known as Verity, and you will see Verity still used in many of the interfaces described in the following procedures.
- If your Content Engine runs on Windows, then the machines in your Content Search Engine configuration must run on Windows. If your Content Engine runs on UNIX, then the machines in your Content Search Engine configuration must run on UNIX, but it doesn't have to be the same UNIX type.
- Where machine name variables are required, IP addresses will not validate. A valid name must be entered.
- If you unimport the style set, the original files will be deleted from your system. In this scenario, if you wish to re-import the style set, recover it from your installation package. In order to avoid this situation, you can either enter a unique name for the Style Set Alias during the initial Content Search Engine (Autonomy K2) installation, or make a backup copy of the original style set. If you enter a unique name for the style set during installation, ensure you use that name when you configure Content Engine for Content-Based Retrieval.
- Stop word files can be used to increase performance by about 30%. You can place the `style.stp` file into the `stylefiles` directory to list words you do not want full-text indexed, for example, short words such as `a`, `the`, or `and`. However, any word in the stop word file cannot be searched. See the K2 documentation for more details. To create a stop word file you can typically copy the `vdk30.stp` file from either the main K2 install directory or the foreign language locales package over to the main `stylefile` directory, and then rename the file `style.stp`. You must do this copy operation before you create collections. Because indexing is case sensitive, the `style.stp` file should include lower-case and upper-case versions of words in the stop word list. For example, use `"the"`, `"The"` and `"THE"` if you think that all of these might be encountered in a search.

## Upgrading Content Search Engine (UNIX)

You must install the K2 Master Administration Server software first. The Master Administration Server dashboard is the central control point for configuring Content Search Engine for single-server or multiserver installations.

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

To install interactively on UNIX, X-Terminal must be installed.

You must designate each installation as either a Master Administration Server software installation or an Administration Server software installation. Only one K2 Master Administration Server can be installed for each Content Engine domain.

**Remember:** Most processes for the Autonomy K2 software will run as `k2_os_user`. However, the `vspget` process must run as root.

To install Content Search Engine on UNIX:

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 Search Engine values, filter by **CSE Installer** in the **Installation or Configuration Program** column.


2. Log on to the machine as *k2\_os\_user*.
3. Set the following environment variable and place the entry in the .profile file for *k2\_os\_user*.
 

```
JAVA_HOME=java_(JDK)_install_path/jdkversion
export JAVA_HOME
```
4. Start the interactive or silent Content Search Engine installation:
  1. "Upgrading Content Search Engine interactively (UNIX)"  
To upgrade Content Search Engine interactively, you must run an installation program wizard.
  2. "Upgrading Content Search Engine silently (UNIX)" on page 290  
When you upgrade Content Search Engine silently, you run a command in the Content Search Engine software package that references parameters in an installation text file.
  3. "Setting environment variables for Content Search Engine (UNIX)" on page 291  
Content Search Engine requires environment variables to be added to the .profile file of the Autonomy K2 operating system user.
  4. "Starting or stopping the autonomy K2 services on UNIX" on page 291  
You can manually start or stop the Autonomy K2 services by issuing different commands according to your environment.

#### Related concepts

 Content Search Engine accounts

For details on accounts and required permissions, see "Creating accounts for Content Search Engine" in *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*.

#### Upgrading Content Search Engine interactively (UNIX):

To upgrade Content Search Engine interactively, you must run an installation program wizard.

An X terminal must be installed on the Content Search Engine server to run the interactive installation program.

To upgrade Content Search Engine:

1. Run the installation program:

Platform	Command
HPUX	P8CSE-4.5.1.0-HPUX.BIN
AIX	P8CSE-4.5.1.0-AIX.BIN
Solaris	P8CSE-4.5.1.0-SOL.BIN
Linux	P8CSE-4.5.1.0-LINUX.BIN

2. Complete the installation screens using the values in your worksheet.

3. Review the following Content Search Engine log files for installation errors. The files are located in the `verity` directory of the installation path:
  - `cse_install_path /verity/cse_install_log_4_5_1.txt`
  - `cse_install_path /verity/vconfig.log`
4. Access the host machine and log on as a user with root privileges.
5. Enter the following commands to set the setuid bit for the `vspget` program so that the service runs as root:
 

```
chown root verity_install_path/k2/_platform/bin/vspget
chmod u+s verity_install_path/k2/_platform/bin/vspget
```

 Replace `_platform` with the following directory:

Platform	Directory
AIX	_rs6k43
HPUX	_hpux
Solaris	_ssol26
Linux	_ilnx21

### Upgrading Content Search Engine silently (UNIX):

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

To upgrade Content Search Engine silently:

1. Access the IBM FileNet Content Search Engine installation package.
2. Edit the `CSE_silent_install.txt` file for your installation using the values from your worksheet.
3. Run the following command: Run the following command:

Platform	Command
HPUX	<code>P8CSE-4.5.1.0-HPUX.BIN -f CSE_silent_install.txt -i silent</code>
AIX	<code>P8CSE-4.5.1.0-AIX.BIN -f CSE_silent_install.txt -i silent</code>
Linux	<code>P8CSE-4.5.1.0-LINUX.BIN -f CSE_silent_install.txt -i silent</code>
Solaris	<code>P8CSE-4.5.1.0-SOL.BIN -f CSE_silent_install.txt -i silent</code>

4. Review the following Content Search Engine log files for installation errors. The files are located in the `verity` directory of the installation path:
  - `cse_install_path /verity/cse_install_log_4_5_1.txt`
  - `cse_install_path /verity/vconfig.log`
5. Access the host machine and log on as a user with root privileges.
6. Enter the following commands to set the setuid bit for the `vspget` program so that the service runs as root:
 

```
chown root verity_install_path/k2/_platform/bin/vspget
chmod u+s verity_install_path/k2/_platform/bin/vspget
```

 Replace `_platform` with the following directory:

Platform	Directory
AIX	_rs6k43
HPUX	_hpux
Solaris	_ssol26
Linux	_ilnx21

### Setting environment variables for Content Search Engine (UNIX):

Content Search Engine requires environment variables to be added to the `.profile` file of the Autonomy K2 operating system user.

To set environment variables:

In the `.profile` file for `k2_os_user`, set the `PATH`, `SHLIB_PATH`, `LIBPATH`, and `LD_LIBRARY_PATH` environment variables (depending on your operating system), each on its own line, without line breaks.

**Important:** If your `.profile` file has a line containing `set -u` that appears before the lines involving `PATH`, `SHLIB_PATH`, `LIBPATH`, or `LD_LIBRARY_PATH`, you must do one of the following edits before setting the environment variables:

- Remove the line containing `set -u` from the `.profile` file.
- Move the line containing `set -u` to a point in the `.profile` file below the lines involving `PATH`, `SHLIB_PATH`, `LIBPATH`, or `LD_LIBRARY_PATH`.

#### AIX

```
PATH=$PATH:verity_install_path/k2/_rs6k43/bin
export PATH
LIBPATH=$LIBPATH:verity_install_path/k2/_rs6k43/bin
export LIBPATH
```

#### HP-UX

```
PATH=$PATH:verity_install_path/k2/_hpux/bin
export PATH
SHLIB_PATH=$SHLIB_PATH:verity_install_path/k2/_hpux/bin
export SHLIB_PATH
```

#### Linux

```
PATH=$PATH:verity_install_path/k2/_ilnx21/bin
export PATH
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:verity_install_path/k2/_ilnx21/bin
export LD_LIBRARY_PATH
```

#### Solaris

```
PATH=$PATH:verity_install_path/k2/_ssol26/bin
export PATH
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:verity_install_path/k2/_ssol26/bin
export LD_LIBRARY_PATH
```

### Starting or stopping the autonomy K2 services on UNIX:

You can manually start or stop the Autonomy K2 services by issuing different commands according to your environment.

To manually start or stop the Autonomy K2 services, use the following commands, according to your environment. (Each command is to be typed on one line.)

Option	Description
HP-UX	Start services: <pre>nohup verity_install_path/k2/_hpux/bin/k2adminstart &amp;</pre> Stop services: <pre>verity_install_path/k2/_hpux/bin/k2adminstop</pre>
AIX	Start services: <pre>nohup verity_install_path/k2/_rs6k43/bin/k2adminstart &amp;</pre> Stop services: <pre>verity_install_path/k2/_rs6k43/bin/k2adminstop</pre>
Solaris	Start services: <pre>nohup verity_install_path/k2/_ssol26/bin/k2adminstart &amp;</pre> Stop services: <pre>verity_install_path/k2/_ssol26/bin/k2adminstop</pre>
Linux	Start services: <pre>nohup verity_install_path/k2/_ilnx21/bin/k2adminstart &amp;</pre> Stop services: <pre>verity_install_path/k2/_ilnx21/bin/k2adminstop</pre>

## Upgrading Content Search Engine (Windows)

Install and configure IBM FileNet P8 Content Search Engine,

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

Install the Autonomy K2 software on each machine in your Content Search Engine configuration. You must complete a K2 Master Administration Server software installation before you can add any additional K2 Administration Server installations. The Master Administration Server dashboard is the central control point for configuring all additional Administration Servers that are part of the Content Search Engine configuration.

You must designate each installation as either a Master Administration Server software installation or an Administration Server software installation.

**Important:** Only one K2 Master Administration Server can be installed for each Content Engine domain.

To install Autonomy K2:

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 Search Engine values, filter by **CSE Installer** in the **Installation or Configuration Program** column.

2. Access the host machine and log on as *k2\_os\_user*.

**Important:** Ensure *k2\_os\_user* has administrator privileges on this machine.

3. Set the JAVA\_HOME environment variable as follows:
  - a. Open the Windows Control Panel.
  - b. Choose **System**.
  - c. Click the **Advanced** tab.
  - d. Click **Environment Variables**.
  - e. Click **New** under System Variables.
  - f. Set the variable information as follows:  
Variable name: *JAVA\_HOME*  
Variable value: *Java (JDK) install path*

**Important:** The installer will not allow you proceed with the installation until the JAVA\_HOME environment variable is set.

4. Access the IBM FileNet Content Search Engine installation package.
5. Start the Content Search Engine installation, choosing either the interactive or silent method.

“Upgrading Content Search Engine interactively (Windows)”

To upgrade Content Search Engine interactively, you must run an installation program wizard.


“Upgrading Content Search Engine silently (Windows)” on page 294

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

### Related concepts

 Content Search Engine 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*.

### Upgrading Content Search Engine interactively (Windows):

To upgrade Content Search Engine interactively, you must run an installation program wizard.

To upgrade Content Search Engine interactively:

1. Run the P8CSE-4.5.1.0-WIN.EXE file.
2. Complete the installation screens using the values from your worksheet.
3. Review the following Content Search Engine log files for installation errors. The files are located in the verity directory of the install path:
  - *cse\_install\_path\verity\cse\_install\_log\_4\_5\_1.txt*
  - *cse\_install\_path\verity\vconfig.log*
4. Verify that the following Autonomy K2 services are installed and running on your Content Search Engine machine after the installation is complete:
  - Verity K2 6.2.1 Administration Server service
  - Verity K2 Administration Web Server service (Tomcat server)



## Upgrading Content Search Engine silently (Windows):

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

To upgrade Content Search Engine silently:

1. Run the P8CSE-4.5.1.0-WIN.EXE file.
2. Complete the installation screens using the values from your worksheet.
3. Review the following Content Search Engine log files for installation errors. The files are located in the `verity` directory of the install path:
  - `cse_install_path \verity\cse_install_log_4_5_1.txt`
  - `cse_install_path \verity\vconfig.log`
4. Verify that the following Autonomy K2 services are installed and running on your Content Search Engine machine after the installation is complete:
  - Verity K2 6.2.1 Administration Server service
  - Verity K2 Administration Web Server service (Tomcat server)

## Updating the style file of user fields

You need to edit the Autonomy K2 style file of user fields to add a data field definition for storing the partitioning value of a document.

To edit the style file:

1. Navigate to the directory in the Content Search Engine software that contains the `style.ufl` file:

### Windows

```
verity_install_path\data\stylesets\FileNet_FileSystem_PushAPI
```

**UNIX** `verity_install_path/data/stylesets/FileNet_FileSystem_PushAPI`

2. Open the Autonomy K2 style file of user fields, `style.ufl`, for editing.
3. If it is not already present, add the CEMP definition at the bottom of the file:

```
data-table: fce
{
 fixwidth: cemp_partition_date 4 unsigned-integer
}
```

4. Save your edits and close the file.

## Configuring Content Search Engine

You can configure services required on the K2 Master Administration Server, and on additional Administration Servers you might install for IBM FileNet P8 Content Search Engine. All servers are configured through the Master Administration Server Dashboard.

- When you name the servers that you create, it is a best practice to indicate the type of server in the server name. Otherwise, when you configure Content Engine by using Enterprise Manager, it can be difficult to determine which server to select for an action. For example, use `server_name_broker` to indicate a Broker Server service.
- Ensure you carefully record the server names, ports and settings that you define. Much of the following information will be required later when you configure the IBM FileNet P8 Content Engine for Content-Based Retrieval later in this guide.
- A range of ports is recommended in the Verity K2 Dashboard for each service you create. You do not have to choose a port number from within that range.

- Repeat the related step in the procedure below to add additional services. Some guidelines must be adhered to when adding additional services:
  - Multiple brokers can be assigned, so that if one goes down the others will be used. However, each broker must have all K2 Servers (search servers) attached that are needed to access collections (index areas). The Content Engine Server will not call multiple brokers and merge the results.
  - If you add additional Index Servers and K2 Servers (search servers), they will not be activated until you enable them through Enterprise Manager. See “Configuring Content Engine for content-based retrieval” on page 98 for details.
  - Each K2 Administration Server must contain a Ticket Server for Content Engine.
  - For good stability and performance, Broker Servers must be attached to local Ticket Servers for security on each machine.
- In the following procedure, import the IBM FileNet Styleset only once, regardless how many K2 Administration Server machines you install.

To configure Content Search Engine:

1. (Optional) Configure the Autonomy K2 Dashboard to use SSL security. The Autonomy K2 Dashboard web application, by default, uses a non-SSL Web site and sends username and password information in plain text. For information on how to modify your Tomcat web applications to use SSL, access the following address:  
<http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html>
2. Access the K2 Dashboard by launching your browser and entering:  
[http://Master Administration Server hostname:9990/verity\\_dashboard/main.jsp](http://Master Administration Server hostname:9990/verity_dashboard/main.jsp)
3. Create a K2 Index Server, as follows :
  - a. Click **K2 Index Servers** under **System View**.
  - b. Click **Add a K2 Index Server** on the K2 Index Server Summary page.
  - c. Enter the following information on the Configure basic settings for the new K2 Index Server page:
    - Service Alias: *server\_name\_index\_server*
    - Port: 9960 - 9979 (suggested range)
  - d. Click **Next** to continue with the installation.
  - e. Enter the following information on the Configure threads for the K2 Index Server page:
    - Synchronous Threads: 25
    - Asynchronous Threads: 3
    - Access Type: *Authorized Administrator*
  - f. Click **Finish** to continue with the installation.
4. Set the Index Server logging properties:
  - a. Click the Index Server, under System View, that you want to adjust.
  - b. Click **Edit Properties** under Actions.
  - c. Click the **Logging** tab.
  - d. For Status Log Nominal Size, enter the following value:  
 9000 kilobytes
  - e. Click **Modify**.
5. Create a K2 Broker Server:

- a. Click **K2 Brokers** under **System View**.
  - b. Click **Add a K2 Broker** on the K2 Broker Summary page.
  - c. Enter the following information on the Configure basic settings for the new K2 Broker page:
    - Service Alias: *server\_name\_broker*
    - Port: 9900 - 9909 (suggested range)
  - d. Click **Finish**.
6. Create a K2 Server (search server) and attach the Broker:
    - a. Click **K2 Servers** under **System View**.
    - b. Click **Add a K2 Server** under **Actions** on the K2 Server Summary page.
    - c. Enter the following information on the Configure basic settings for the new K2 Server page:
      - Service Alias: *server\_name\_search\_server*
      - Port: 9920 - 9949 (suggested range)
    - d. Click **Next**.
    - e. Click **Next** on the Set security options for this service page.
    - f. Enter the following information on the Attach to K2 Brokers page:
      - Select the K2 Brokers that will provide access to this service: Select the K2 Broker you created in step 3 from the drop-down menu, *server\_name\_broker*.
    - g. Click **Finish**.
  7. Import the IBM FileNet Styleset.
    - a. Click **Collections** under System View.
    - b. Click **Manage Style Sets** under **Actions** on the Collection Summary page.
    - c. Click **Import** on the Manage Style Sets page (top right).
    - d. Enter the following information on the Import page:
      - Style Set Alias: *FileNet\_FileSystem\_PushAPI*
      - Gateway Type: --Auto-detect--
      - Source Administration Server. If multiple servers are installed, choose the server to which you will import the Styleset.
      - Source Path:

**Windows**

```
verity_install_path\data\stylesets\
FileNet_FileSystem_PushAPI
```

**UNIX** *verity\_install\_path/data/stylesets/  
FileNet\_FileSystem\_PushAPI*

- e. Click **Import**.

**Tip:** The K2 Dashboard displays a notification that the StyleSet Editor web application cannot be accessed. This message can be ignored as it relates to a function that is not used by Content Search Engine.

8. Navigate to the source path you specified in the preceding step and complete the following substeps:
  - a. Open the file *style.ufl* for editing.
  - b. If it is not already present, add the CEMP definition at the bottom of the file:

```

data-table: fce
{
fixwidth: cemp_partition_date 4 unsigned-integer
}

```

- c. Save and close the file.
9. Create a K2 Ticket Server.
  - a. Click **K2 Ticket Servers** under **System View**.
  - b. Click **Add a K2 Ticket Server** under **Actions** on the K2 Ticket Server Summary page.
  - c. Enter the following information on the Configure basic settings for the new K2 Ticket Server page:
    - Service Alias: *server\_name \_ticket\_server*
    - Port: 9910 - 9919 (recommended range)
  - d. Click **Next**.
  - e. Enter the following information on the Configure the login module to use with this K2 Ticket Server page:
    - Select which Login Module type to use with this K2 Ticket Server:
      - Windows
      - UNIX

**Restriction:** LDAP Ticket Servers are not currently supported.

    - Default Domain (Windows only): Enter the domain on which this K2 Server is authenticated. If the server is in a workgroup, leave this field blank.
  - f. Click **Next**.
  - g. Enter the following information on the Configure the persistent store module to use with this K2 Ticket Server page:
    - Select the Persistent Store Module type to use with this K2 Ticket Server: Choose File and Memory.
  - h. Click **Finish**.
  - i. (Windows only) Specify local login settings:
    - 1) Click **Edit Properties**.
    - 2) Click Windows Login Module.
    - 3) Select the **Use Local Credentials** check box.
    - 4) Clear the **Enable Built-in Groups** check box.
    - 5) Click **Modify**.
10. Set Autonomy K2 Administration Security.
  - a. Click the K2 Ticket Server you created.
  - b. Click **Manage Administration Security** under Actions.
  - c. Enter the following information on the Manage Administration Security page:
    - Select a K2 Ticket Server to configure for administration security: From the drop-down menu, select the K2 Ticket Server you just created.
    - User Name: Enter the *k2\_os\_user*. For UNIX installs, this is the user you logged in as to run the installation.
    - Password: Enter the authentication password.
    - Default Domain (Windows only): Enter the domain on which this user and K2 Server are authenticated. If the server is in a workgroup, leave this field blank.

d. Click **Modify**.

The K2 software will authenticate the user based on the information you entered. If the check fails, an error message will indicate what failed and request that you re-enter the information.

If administrator access is successful, Autonomy K2 will close the Dashboard and require that you log on again as the Dashboard Administrator to complete the configuration.

11. Launch the K2 Dashboard and log on.

12. Restart K2 services:

- a. Under **Notifications** on the K2 Dashboard Home page, a number of servers are listed as requiring a restart. Click **Start/Stop this Service** to access the settings page and follow the instructions listed there. You must choose **Full Restart**.
- b. Click **Home** in the top-left corner of the page after each restart to view the remaining notifications. Repeat the process until there are no notifications remaining.

13. Enable additional K2 Admin Users (optional).

- a. From the K2 Dashboard home page, click **Administration Servers**.
- b. Click **Manage K2 Administrative Users**.
- c. Click **Add User** on the Manage K2 Administrative Users page.
- d. Enter the name of an authenticated user on the directory service that you want to make a K2 Administrator and click **Add**.

14. Enable security on the K2 services you have created.

- a. From the K2 Dashboard home page, click **K2 Ticket Servers**.
- b. Click your ticket server *server\_name\_ticket\_server*.
- c. Click **Manage K2 Broker/K2 Server Security** in the Services Secured by this K2 Ticket Server section of the page (bottom right).
- d. Click **K2 Servers** on the Manage K2 Broker/K2 Server Security page.
- e. Click the service you just created which is listed in the window on the right to enable security.

**Important:** If you have a multiserver configuration, numerous services, installed on other machines, will be listed also. Select only the service to which you want to attach a broker. Brokers must be attached to local ticket servers for Content Search Engine.

- f. Click **K2 Brokers** on the Manage K2 Broker/K2 Server Security page.
- g. Click the Broker in the window on the right that you want to attach to the local K2 ticket server you selected above.
- h. Click **Modify** to save your changes.

15. Restart K2 services, as follows:

- a. Click **Home** in the top left corner of the page.
- b. Under **Notifications** on the Verity K2 Dashboard Home page, a number of servers are listed as requiring a restart. Click **Start/Stop this Service** to access the settings page and follow the instructions listed there. You must choose **Full Restart**.

Click **Home** in the top left corner of the page after each restart to view the remaining notifications. Repeat the process until there are no notifications remaining.

1. "Configuring services on administration servers" on page 299

Use this procedure to create and configure services on specific Content Search

Engine machines (Administration Servers), other than the Master Administration Server. Services for all machines in your Content Search Engine configuration are configured through the Master Administration Server Dashboard.

### Related concepts

 Content Search Engine accounts

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

### Configuring services on administration servers:

Use this procedure to create and configure services on specific Content Search Engine machines (Administration Servers), other than the Master Administration Server. Services for all machines in your Content Search Engine configuration are configured through the Master Administration Server Dashboard.

1. Click **Administration Servers** under **System View**.
2. Click the Administration Server to which you want to add services.
3. Click **Add a Service** under K2 Services on this Administration Server.
4. Select the service you want to add.
5. Follow the instructions and guidelines for the appropriate service in the To configure Content Search Engine procedure above to complete the service addition.

### Configuring Autonomy K2 for version 4.5.1 index areas

For performance reasons, it is recommended that you create one collections directory for each index area you create in IBM FileNet P8 Content Engine. Each collections directory you create must be set to provide proper security access. The path to both the collections directory and collections temp directory must be entered in the index area properties when you create them.

Security and communication between Autonomy K2, Content Engine, and the collections directory is handled through the user accounts and permissions provided to those accounts. For detailed information on security, see the IBM FileNet P8 help topic **System Administration** → **Enterprise-wide Administration** → **FileNet P8 Security** → **Authorization** → **Security for integrated components and third-party products** → **Autonomy K2 Server**.

1. "Collections directory requirements for Content Search Engine" on page 300  
The task of creating a collections directory includes setting up security permissions to allow read and write access.
2. "Windows-specific options" on page 301  
You can configure a read-only Autonomy K2 Administration server which will remotely read collections (note that you cannot have a second K2 Administration server that writes the collections). To do this, you must map a drive on the read-only Administration server to the file system on the Autonomy K2 machine that writes collections.
3. "Completing the upgrade" on page 302  
Completing the upgrade of Content Search Engine is part of the process for upgrading Content Engine.

## Related concepts

### Content Search Engine 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 parameter values, see *Plan and Prepare Your Environment for IBM FileNet P8*.

## Collections directory requirements for Content Search Engine:

The task of creating a collections directory includes setting up security permissions to allow read and write access.

**Important:** Contrary to information outlined in the Autonomy-supplied documentation set, remote collections are not supported for use with IBM FileNet Content Search Engine. Collections must be written locally to the Autonomy K2 server. Using a remote-mounted disk that is accessed using the network (NFS, PCNFS, or CIFS) causes stability problems under load and corrupt your collections. Any existing configurations that contain non-local collections directories must be reconfigured.

To create a collections directory:

1. Create a directory in which to store collections (VerityIndexArea.RootDirectoryPath). This directory must be located on a disk that is local to the Verity server. Set permissions to allow access to the *k2\_os\_user*.  
This path must be local to the index server that is assigned to write collections.
2. Create a temp directory (VerityIndexArea.TempDirectoryPath) which is used by the K2 Index Server and Content Engine Server during operations.  
Content Engine and the Autonomy K2 servers, the K2 Administration Server and Content Engine must be on the same machine or on a network mounted file system.
3. Provide read/write access to the collections directory for Autonomy K2 by entering the full path to the location and record the temp collections path.

Option	Description
Windows	<ol style="list-style-type: none"><li>1. Open the following K2 configuration file in a text editor (default path shown): <code>verity_install_path\k2\common\verity.cfg</code></li><li>2. Modify the next available alias settings by adding the collections path, where new collections are written. For example, change <code>alias6</code>, <code>mapping6</code>, and <code>dirmode6</code> to the following settings: <code>alias6=path1</code> <code>mapping6=C:\Collections_Directory</code> <code>dirmode6=wr</code></li></ol>



Option	Description
UNIX	<ol style="list-style-type: none"> <li data-bbox="966 226 1451 344">1. Open the following K2 configuration file in a text editor (default path shown): <i>verity_install_path/k2/common/verity.cfg</i></li> <li data-bbox="966 352 1451 554">2. Modify the next available alias settings by adding the collections path. For example, change <i>alias6</i>, <i>mapping6</i>, and <i>dirmode6</i> to the following settings:  <i>alias6=path1</i> <i>mapping6=/Collections_Directory_Path</i> <i>dirmode6=wr</i></li> </ol> <p data-bbox="1003 567 1451 621">The <i>Collections_Directory_Path</i> must be a local path and not a mount point.</p>

4. Set file store access. Each file store that is full text indexed must be accessible by the Autonomy K2 server that performs the full text indexing. Permissions on the file store must be set the same as the permissions on the collections directories. Having the same permissions allows both the Content Engine Operating System User and the Verity Operating System User to access them. The names of the file store directories must also be the same on each server that access the directories.

Although we are mapping remote collections, which are not supported, indexing is not run on these indexes. The mapping is used to close the collections.

#### Windows-specific options:

You can configure a read-only Autonomy K2 Administration server which will remotely read collections (note that you cannot have a second K2 Administration server that writes the collections). To do this, you must map a drive on the read-only Administration server to the file system on the Autonomy K2 machine that writes collections.

To do this, share the Autonomy K2 machine's collections drive (for example, *D:\*) as some name other than *D\$* , because you can't set permissions on *D\$* . For example, set it as *DDrive* .

Map the *D:\* drive on the read-only Autonomy K2 machine to *\\servername\DDrive* .

Now *D:\collections* on the read-only Autonomy K2 machine references the same file system as the *D:\* drive on the Autonomy K2 machine that writes the collections.

By default, the *k2admin.exe* program on the read-only Autonomy K2 machine runs as a Windows service. This is a problem because Windows services can not mount mapped drives.

One solution to this problem is to run the *k2admin.exe* program from a command line instead, so that it doesn't run as a Windows service. To launch the service manually from a command line on a default installation, run the following command:

```
C:\Program
Files\verity\k2_61\k2_nti40\bin\k2admin.exe" -cfg "C:\Program
Files\verity\k2_61\k2\common\verity.cfg
```

**Important:** Only the Verity K2 6.1.1 Administration Server service (*k2admin.exe*) must be started this way. The Verity Administration Web Server might be left as a Windows service.

Another solution is to use a tool like the *svrany.exe* program (supplied as part of the Windows Resource kit) to run a *.cmd* file that first maps the drives, and then issues the command above to start the *k2admin.exe* service. The command to map drives, using the above example, is:

```
net use D: \\servername\DDrive
```

Independent software vendor products are available that function the same as the *svrany.exe* program.

Although the *svrany.exe* program will start the service correctly, it cannot stop the service. You must use the Autonomy *rcadmin* command line tool to stop the service, or use TaskManager and stop all the processes that start with the prefix *k2*.

To use the Autonomy *rcadmin* program from a command line:

1. Access a command line and type the following command: *rcadmin*
2. Enter the following command to log on: *login k2\_os\_user*
3. Enter the following command to initiate the shutdown: *adminsignal*
4. Enter one of the following responses to the Type of Signal query:
  - 2 - Shutdown
  - 3 - WS Refresh
  - 4 - Restart all servers

### Completing the upgrade:

Completing the upgrade of Content Search Engine is part of the process for upgrading Content Engine.

The remaining steps required to complete an upgrade of Content Search Engine must be completed as part of the overall Content Engine upgrade and are outlined at the appropriate locations later in this guide.

## Updating the CFS-IS settings

If Content Federation Services for Image Services (CFS-IS) is in your version 3.5.2 system, then you must enable the Image Services dispatcher. You must also modify the default map between CFS-IS and the object stores in the FileNet P8 domain.

To update the CFS-IS settings:

1. Start Enterprise Manager if it is not already running.
2. Right-click the Enterprise Manager root node in the navigation tree (left pane), and select **Properties**.
3. Click the **IS Import Agent** tab, select the **Enable Dispatcher** check box, and then click **OK**.
4. Start the Image Services Remote Admin Console by selecting **Start** → **Programs** → **FileNet P8 Platform** → **IS Remote Admin Console**.
5. For each object store that participates in CFS-IS federation, complete the following substeps:

- a. Select **Applications** → **IS Catalog Export Tool**. The Default Mappings window displays the Image Services document class that is mapped to a FileNet P8 domain/object store combination.
  - b. Select the *document class name* and click **Remove**, and then click **OK**.
  - c. Modify the `f_ce_domain_guid` and `f_ce_domain_name` columns in the `ce_id_map` table on the IS database to match the new Content Engine version 4.5.1 domain GUID and domain name. For example:
 

```
UPDATE ce_id_map SET f_ce_domain_guid = 'new_domain_guid' ,
f_ce_domain_name = 'new_domain_name'
where f_ce_os_name = 'object_store_name';
```

 Use Enterprise Manager to determine the *new\_domain\_guid* and *new\_domain\_name* values. Right-click the **P8 Domain node**, and select **Properties**. The ID property is the domain GUID.
6. Restart Image Services:
    - To restart Image Services by using the graphical user interface, start FileNet Image Services Task Manager and click **Restart**.
    - To restart Image Services from a command line, run the following commands:
 

```
initfnsw -y stop
killfnsw -DyAS
initfnsw start
```
  7. For each object store that participates in CFS-IS federation, configure the Image Services documentation class for export to Content Engine.
    - a. On the main Remote Admin Console screen, select **Applications** → **IS Catalog Export Tool**.
    - b. From the **CE Configured IS Doc Classes** menu, select the IS document class whose index properties you want to export to Content Engine.
    - c. From the Available CE Object Store Mappings pane, select the Content Engine domain and object store that you want to export to Content Engine.
    - d. Click **Set Default Map**.
  8. Stop and start Content Engine.
  9. Verify your property mappings.
    - a. Start Enterprise Manager if it is not already running.
    - b. Right-click the *object store node* in the navigation tree (left pane), and select **Properties**.
    - c. Click the **Content Federation** tab.
    - d. Select your *class mapping name* and click **Add/Edit**.
    - e. Select **Current Class Mappings**, and click **Map Properties**.
    - f. Verify your property mappings.
    - g. Click **OK**.
    - h. Close Enterprise Manager.

## Upgrading Content Engine data

You must upgrade your current Content Engine data (GCD, addons, fixed content devices, object stores, and related information).

There are two tools available to you for upgrading Content Engine data: the IBM FileNet Content Engine Upgrader tool and IBM FileNet Content Engine Upgrader Web Tool. The Content Engine Upgrader tool has both a graphical user interface (GUI) and a command-line interface (CLI). Content Engine Web Upgrade Tool has

only a graphical user interface. Choose a tool for upgrading Content Engine data based upon the criteria in the following table:

Interface to be used	Current state of the object stores	Upgrade tool to use
GUI	All object stores are at version 3.5.2.	Content Engine Web Upgrade Tool or Content Engine Upgrader tool
GUI	Some object stores at version 4.5.1 were upgraded using Content Engine Upgrader tool; other object stores in the same domain are still at version 3.5.2.	Content Engine Upgrader tool
GUI	Some object stores at version 4.5.1 were upgraded using Content Engine Web Upgrade Tool; other object stores in the same domain are still at version 3.5.2	Content Engine Web Upgrade Tool
CLI	Not applicable	Content Engine Upgrader tool

Whichever tool you use, keep in mind the following guidelines as you prepare to upgrade the Content Engine data:

- It is not necessary to check in checked-out documents before running either upgrade tool.
  - If the maximum heap size of the JVM is 1 GB or more, do not run an upgrade tool on the same machine where any other major application (such as a database) is running unless the machine has at least 2 GB of RAM.
  - If you use Content Engine Web Upgrade Tool to upgrade your Content Engine data, you must deploy it on the same Java Virtual Machine where version 4.5.1 of Content Engine is deployed.
  - If you are upgrading an IBM FileNet P8 environment with many object stores, use the following approach:
    - Upgrade fewer than 20 object stores at a time.
    - For best performance when Content Engine is deployed on a web application server with a 32-bit JVM, restrict each version 4.5.1 FileNet P8 domain to 50 or fewer object stores. If the version 3.5.2 FileNet P8 domains contain more than 50 object stores, consider partitioning them into multiple 4.5.1 FileNet P8 domains during the upgrade process.
    - Ensure that the version 3.5.2 object stores with the same basic set of system objects (for file stores, fixed file stores, and related objects) are upgraded into the same 4.5.1 FileNet P8 domain.
  - The time to upgrade object stores from version 3.5.2 depends on the number of documents the object store contains, the database type, and the resources of the machine on which the database system runs. If you are upgrading version 3.5.2 object stores that contain more than a million documents or a million custom objects, the Upgrader tool can take more than an hour to complete the upgrade.
  - For non-English support relating to collections, see *IBM FileNet P8 Non-English Support Guide*.
1. “Upgrading Content Engine data using Content Engine Web Upgrade Tool” on page 305

Use Content Engine Web Upgrade Tool to validate and upgrade your version 3.5.2 FileNet P8 domain and object stores.

2. “Upgrading Content Engine data using Content Engine Upgrader tool” on page 317

Use Content Engine Upgrader tool to upgrade your version 3.5.2 FileNet P8 domain and object stores if you cannot use Content Engine Web Upgrade Tool.

#### Related information



Product documentation for IBM FileNet P8 Platform

Download the IBM FileNet P8 Non-English Support Guide, as well as PDF's of the rest of the IBM FileNet P8 Platform documentation.

## Upgrading Content Engine data using Content Engine Web Upgrade Tool

Use Content Engine Web Upgrade Tool to validate and upgrade your version 3.5.2 FileNet P8 domain and object stores.

Content Engine Web Upgrade Tool runs on the machine where Content Engine is deployed. You run the tool in two phases: validation and then upgrade.

The validation phase determines whether your object stores and related data are ready for upgrade. You can select all the object stores for validation in one step, or you can select subsets of them for validation in several steps. During the first validation step, even if you have not selected any object stores, Content Engine Web Upgrade Tool validates (by default) the GCD, domain addons, and fixed content devices. During a validation step Content Engine Web Upgrade Tool does not stop at errors; it proceeds until it has validated all the selected object stores. If an object store fails validation, you must edit its associated data and then run the validation again until it succeeds.

The upgrade phase upgrades the successfully validated object stores. You can select all the object stores for upgrading in one step, or you can select subsets of them for upgrading in several steps. The first time you run the upgrade step, even if you have not selected any object stores, Content Engine Web Upgrade Tool upgrades (by default) the GCD, domain addons, and fixed content devices. During an upgrade step Content Engine Web Upgrade Tool stops at the first error. If an object store upgrade fails, you must edit its associated data and then upgrade it again until it succeeds.

“Deploying Content Engine Web Upgrade Tool” on page 306

You need to deploy Content Engine Web Upgrade Tool before you can upgrade your Content Engine data.

“Backing up the version 4.5.1 GCD database” on page 309

You need to back up your version 4.5.1 GCD database before you start upgrading Content Engine data so that in case the upgrade fails, you can recover your original system environment.

“Starting Content Engine Web Upgrade Tool” on page 309

To use Content Engine Web Upgrade Tool, you browse to the machine where the tool is running.

“Upgrading a version 3.5.2 FileNet P8 domain into a new version 4.5.1 FileNet P8 domain” on page 310

You have a new version 4.5.1 FileNet P8 domain and are upgrading version 3.5.2 object stores into it.

“Upgrading a version 3.5.2 FileNet P8 domain into an existing version 4.5.1 FileNet P8 domain” on page 313

You have an existing version 4.5.1 FileNet P8 domain (which already contains object stores) and are upgrading version 3.5.2 object stores into it.

### Deploying Content Engine Web Upgrade Tool:

You need to deploy Content Engine Web Upgrade Tool before you can upgrade your Content Engine data.

You must deploy Content Engine Web Upgrade Tool on the application server where you installed version 4.5.1 of the Content Engine software. Content Engine Web Upgrade Tool is available as of version 4.5.1 FP2 of Content Engine.

“Deploying Content Engine Web Upgrade Tool (WebSphere Application Server)”

You need to deploy IBM FileNet Content Engine Web Upgrade Tool on the application server where version 4.5.1 of Content Engine is deployed.

“Deploying Content Engine Web Upgrade Tool (Oracle WebLogic Server)” on page 308

You need to deploy IBM FileNet Content Engine Web Upgrade Tool on the application server where version 4.5.1 of Content Engine is deployed.

“Deploying Content Engine Web Upgrade Tool (JBoss Application Server)” on page 308

You need to deploy IBM FileNet Content Engine Web Upgrade Tool on the application server where version 4.5.1 of Content Engine is deployed.

#### *Deploying Content Engine Web Upgrade Tool (WebSphere Application Server):*

You need to deploy IBM FileNet Content Engine Web Upgrade Tool on the application server where version 4.5.1 of Content Engine is deployed.

If Content Engine is deployed on a managed node, you must deploy Content Engine Web Upgrade Tool on the that node. If Content Engine is deployed in a cluster, you must deploy Content Engine Web Upgrade Tool in that cluster.

To deploy IBM FileNet Content Engine Web Upgrade Tool on WebSphere Application Server:

1. Log in as *ce\_install\_user* to the application server machine where you installed version 4.5.1 FP2 or later of the Content Engine software.
2. If you are going to upgrade a large object store or a large number of object stores, it is a best practice to deploy Content Engine Web Upgrade Tool to a Java Virtual Machine that has a heap size of at least 512 MB. If the heap size is less than 512 MB, increase the size as needed.
3. Navigate to the directory that contains the *upgrader.war* file, depending on the operating system where Content Engine is installed:

Option	Description
UNIX	/opt/IBM/FileNet/ContentEngine/lib
Windows	C:\Program Files\IBM\FileNet\ContentEngine\lib

4. In the WebSphere Application Server administrative console, navigate to **Applications** → **Enterprise Applications** and click **Install**.
5. (WebSphere 6.1) Specify the path to the *upgrader.war* file, set the context root to */upgrader*, and complete the following substeps:

- a. In the step to select installation options, set the application name to upgrader.
  - b. If your deployment environment is WebSphere Application Server Network Deployment, select the node or cluster where Content Engine is deployed; otherwise, skip past the step to map modules to servers and the step to map virtual hosts to Web modules.
  - c. Skip to the summary. Click **Finish**, and then click **Save**.
6. (WebSphere 7.0) In the Install New Application page, specify the path to the upgrader.war file, click **Next**, and then click **OK** to confirm the path. Then complete the following substeps:
    - a. In the step to select installation options, set the application name to upgrader.
    - b. If your deployment environment is WebSphere Application Server Network Deployment, select the node or cluster where Content Engine is deployed; otherwise, skip past the step to map modules to servers and the step to map virtual hosts to Web modules.
    - c. In the step to map context roots for Web modules, set the context root to /upgrader.
    - d. Skip to the summary. Click **Finish**, and then click **Save**.
  7. Ensure that the class loader policy is set to Multiple by completing the following substeps on each server where you are deploying the upgrader.war file:
    - a. In the WebSphere Application Server administrative console, navigate to **Servers** → **WebSphere application servers** and click the name of the server where you just deployed the upgrader.war file.
    - b. Click the **Configuration** tab and under Server-specific Application Settings set the Classloader policy to Multiple.
  8. Synchronize nodes if needed.
  9. If your deployment environment is WebSphere Application Server Network Deployment, complete the following substeps:
    - a. Open for editing the deployed version of the config.properties file. You can this file at one of the following locations.

Operating system	Path to config.properties file
UNIX	/opt/IBM/WebSphere/AppServer/profiles/ <i>profile_name</i> /installedApps/ <i>cell_name</i> /upgrader_war.ear/upgrader.war/WEB-INF/classes
Windows	C:\Program Files\IBM\WebSphere\AppServer\profiles\ <i>profile_name</i> \installedApps\ <i>cell_name</i> \upgrader_war.ear\upgrader.war\WEB-INF\classes

- b. Find the line in the file that starts with SOAPConnectorAddress and change the port (the value after the =) to the port number that the deployment manager uses.
10. Navigate back to **Applications** → **Enterprise Applications**, select upgrader, and then click **Start**.



## Related concepts

 Installation and Upgrade Worksheet

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

*Deploying Content Engine Web Upgrade Tool (Oracle WebLogic Server):*

You need to deploy IBM FileNet Content Engine Web Upgrade Tool on the application server where version 4.5.1 of Content Engine is deployed.

To deploy IBM FileNet Content Engine Web Upgrade Tool on Oracle WebLogic Server:

1. Log in as the WebLogic Server administrative user to the administration console on the application server machine where you deployed version 4.5.1 FP2 or later of Content Engine.
2. If you are going to upgrade a large object store or a large number of object stores, it is a best practice to deploy Content Engine Web Upgrade Tool to a Java Virtual Machine that has a heap size of at least 512 MB. If the heap size is less than 512 MB, increase the size as needed.
3. Click **Deployments** in the Domain Structure section of left panel of the administration console.
4. Click **Install** in the right panel.
5. In the Path field, enter the path to the upgrader.war file, depending on the operating system where Content Engine is installed, and then click **Next**.

Option	Description
UNIX	/opt/IBM/FileNet/ContentEngine/lib
Windows	C:\Program Files\IBM\FileNet\ContentEngine\lib

6. Select the check box to install upgrader.war as a deployed application, and then click **Next**.
7. If Content Engine is deployed on only one WebLogic server, skip to step 9.
8. From the Select Deployment Targets page, select the node or cluster where Content Engine is deployed.
9. Specify a name for the deployed application or accept its default value (upgrader), and then click **Next**.
10. Review your choices and click **Finish**.
11. Click **Save**.

## Related concepts

 Installation and Upgrade Worksheet

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

*Deploying Content Engine Web Upgrade Tool (JBoss Application Server):*

You need to deploy IBM FileNet Content Engine Web Upgrade Tool on the application server where version 4.5.1 of Content Engine is deployed.

To deploy IBM FileNet Content Engine Web Upgrade Tool on JBoss Application Server:

1. Log in as `ce_install_user` to the application server machine where you installed version 4.5.1 FP2 or later of the Content Engine software.
2. If you are going to upgrade a large object store or a large number of object stores, it is a best practice to deploy Content Engine Web Upgrade Tool to a Java Virtual Machine that has a heap size of at least 512 MB. If the heap size is less than 512 MB, increase the size as needed.
3. Shut down JBoss if it is running.
4. Navigate to the directory that contains the `upgrader-jb.war` file, depending on the operating system where Content Engine is installed:

Option	Description
UNIX	<code>/opt/IBM/FileNet/ContentEngine/lib</code>
Windows	<code>C:\Program Files\IBM\FileNet\ContentEngine\lib</code>

5. Copy `upgrader-jb.war` to the `jboss_install_dir/server/server_instance_name/deploy` directory.
6. Start JBoss.

#### Related concepts

 [Installation and Upgrade Worksheet](#)

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

#### Backing up the version 4.5.1 GCD database:

You need to back up your version 4.5.1 GCD database before you start upgrading Content Engine data so that in case the upgrade fails, you can recover your original system environment.

To back up your version 4.5.1 GCD database:

User your database administration tools to back up the database that contains the GCD.

#### Starting Content Engine Web Upgrade Tool:

To use Content Engine Web Upgrade Tool, you browse to the machine where the tool is running.

To start Content Engine Web Upgrade Tool:

1. Log on to a machine where version 8.0 of Microsoft Internet Explorer is installed.
2. 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 Web Upgrade Tool values, filter by **CE Web Upgrade Tool** in the **Installation or Configuration Program** column.

3. From the machine you logged on to, browse to the Web site `http://ce_server_name:port_number/upgrader`. `ce_server_name` is the host name of the machine where you run the tool, and `port_number` is the WSI port used by the application server on which Content Engine is deployed. (You cannot browse to the Web site using the HTTPS protocol.)

**Important:** If Content Engine is in a cluster or farm environment, you can run the tool from any node in the environment. Browse directly to the node where the tool is running, rather than using a load balance URL.

4. At the Log In window, log in as *gcd\_admin*, the GCD administrator user. This user must also be an object store administrator with full control permissions on each object store to be upgraded.

**Important:** Do not run more than one instance of Content Engine Web Upgrade Tool at a time.

If this is your first login for the FileNet P8 domain that you are upgrading, continue at step 5. Otherwise, Content Engine Web Upgrade Tool displays the Upgrade Information window, where you can resume validating and upgrading the object stores.

5. Enter the location of the GCD file *sysinit.dat* on the Windows machine where version 3.5.2 of Content Engine is installed. If you previously copied *sysinit.dat* to another location to ensure that it is accessible from a UNIX Content Engine server, you can specify that location instead. Do not rename the file: otherwise, Content Engine Web Upgrade Tool prompts you for a file named *sysinit.dat*.

**Important:** Do not delete the GCD file on the Windows machine where version 3.5.2 of Content Engine is installed.

6. Verify that a file named *upgrade4512.xml* exists. To find the file, navigate to the directory shown in the working directory entry in the right panel of the Upgrade Information page. Then, navigate within that directory to the FileNet/upgrader directory. You might need to edit this file to fix errors that occur during the validation or upgrade phases.
7. Verify that a file named *upgrade\_trace-timestamp.log* is in the FileNet/upgrader/logs directory. Content Engine Web Upgrade Tool creates this file anew each time you log in, and it moves the file from the previous login to the FileNet/upgrader/logs/backup directory. This file records all the validation and upgrade activity.

### **Upgrading a version 3.5.2 FileNet P8 domain into a new version 4.5.1 FileNet P8 domain:**

You have a new version 4.5.1 FileNet P8 domain and are upgrading version 3.5.2 object stores into it.

*“Validating object stores”*

Validation determines whether your object stores and other Content Engine data are ready to be upgraded. You cannot upgrade your object stores until they are successfully validated.

*“Upgrading object stores”* on page 312

You need to upgrade your object stores before they can be made available for use in version 4.5.1 FP2 (or later) of Content Engine.

*Validating object stores:*

Validation determines whether your object stores and other Content Engine data are ready to be upgraded. You cannot upgrade your object stores until they are successfully validated.

To validate object stores:

1. For each fixed content device in the left panel of the Upgrade Information window that needs info (as indicated by its icon in the left panel), select the device and specify the required parameter values in the right panel.

**Important:** The SnapLockPassword parameter value is not stored. If you log off Content Engine Web Upgrade Tool and log back on, you must reenter the value.

2. If Hitachi [SnapLock] or IBM [Tivoli] are listed among the fixed content devices in the left panel, complete the following substeps. Otherwise, Content Engine Web Upgrade Tool does not process them:
  - a. Choose **Tools** → **Edit XML**.
  - b. In the upgrade4512.xml file, replace all occurrences of Unsupported with UpgradeFinished to make Content Engine Web Upgrade Tool ignore these unsupported fixed content devices and fixed file stores (if any) in the object stores you upgrade.
  - c. Click **Save**.
3. Select the object stores to be validated. Initially, all the object stores are selected for validation. You can validate object stores in any order.

If you want to validate object stores individually, select them from the left panel of Content Engine Web Upgrade Tool. If you want to select all the object stores at once, choose **Tools** → **Select All Object Stores**.

You can clear your selections by choosing **Tools** → **Clear All Object Stores**. (The **Clear All Object Stores** menu choice is unavailable until you select at least one object store.)
4. For each object store that you selected to be validated, complete the following substeps:
  - a. In the right panel, specify the required values from your worksheet.
  - b. If the object store uses fixed file stores, set the values for the root directories to their current locations. (The initial values that appear in these fields are from sysinit.dat and are not correct for version 4.5.1 of Content Engine.)
  - c. When you click **Save**, a prompt reminds you to be sure that you chose the correct data sources for the object store. It also reminds to you to verify that you can read from and write to the file stores of the object stores from the Content Engine server.
5. Click **Validate** to validate the object stores that you selected.

Each time you click **Validate**, Content Engine Web Upgrade Tool creates the file validation.log in the directory FileNet/upgrader/logs, and moves the (time-stamped) log file from the previous validation (if any) into the directory FileNet/upgrader/logs/backup. Both directories are relative to the location specified in the working directory on the Upgrade Information page.

Validation errors, such as missing or incorrect parameters, open in the right panel and are also written to validation.log.
6. Select **View** → **Validation Log** to check the validation.log file for errors. The file opens in a scrollable window. Errors are also displayed in the right panel.

You can correct some validation errors within the Content Engine Web Upgrade Tool interface; other errors can be corrected only manually or by using another interface, such as IBM FileNet Enterprise Manager.
7. To correct a validation error within Content Engine Web Upgrade Tool, complete the following substeps:

- a. If the error indicates unspecified or invalid JDBC or JDBC XA data sources, choose the correct data source or fix the data source at the application server.
  - b. If the error is in the file store path, specify the correct path.
  - c. If the error is in the file store path, ensure that the file store exists, and that Content Engine can read and write to the file store. (Content Engine Web Upgrade Tool checks that the destination directory associated with the file store exists and that the inbound directory is empty.)
  - d. Click **Save**.
  - e. Click **Validate** and return to step 6 on page 311.
8. If the validation log indicates an invalid object store state because of pre-upgrade errors (for example, conflicting classes or properties or pending queue items or publishing requests), log on to version 3.5.2 of IBM FileNet Enterprise Manager and fix the error within the Content Engine 3.5.2 domain.
  9. If you successfully validated an object store, you can upgrade it. To validate more object stores, return to step 3 on page 311.

#### *Upgrading object stores:*

You need to upgrade your object stores before they can be made available for use in version 4.5.1 FP2 (or later) of Content Engine.

To upgrade object stores:

1. Select the object stores to be upgrade.

If you want to upgrade object stores individually, select them from the left panel of Content Engine Web Upgrade Tool. If you want to select all the object stores at once, choose **Tools** → **Select All Object Stores**. You can upgrade object stores in any order. In either case, the first set of Content Engine object store that you select for upgrade includes (by default) the GCD, domain addons, and fixed content devices.

You can clear your selections by choosing **Tools** → **Clear All Object Stores**. (The **Clear All Object Stores** menu choice is unavailable until you select at least one object store.

**Tip:** The upgrade log file can get long. For ease in viewing the log, upgrade only one object store at a time.

2. Click **Upgrade**. The right panel displays a log showing the progress of the upgrade.

Each time you click **Upgrade**, Content Engine Web Upgrade Tool creates a file named `upgrade-running.log` in the `FileNet/upgrader/logs` directory, and copies the previous `upgrade-running.log` file to the `upgrader_trace-timestamp.log` file in the `FileNet/upgrader/logs/backup` directory.

After the upgrade starts, you can pause it by clicking **Pause**. The upgrade pauses as soon as it finishes upgrading whatever object store node it is currently processing. To resume the upgrade, click **Resume**.

If you exit the browser in which Content Engine Web Upgrade Tool is running, an upgrade that is in progress continues in the background. If you log back in, you see the upgrade status at its current state in the right panel.

Content Engine Web Upgrade Tool indicates which object store it is upgrading by changing the appearance of the corresponding icon in the left panel. The tool also changes the appearance of each icon to indicate that it has completed the upgrade of an object store.

Content Engine Web Upgrade Tool also puts the most recent upgrade report file `upgrade.htm` into the directory `FileNet/upgrader/reports` and moves the (time-stamped) report file from the previous upgrade into the directory `FileNet/upgrader/reports/backup`. Both directories are relative to the location specified in the working directory on the Upgrade Information page.

3. If Content Engine Web Upgrade Tool detects an error in upgrading an object store, it halts. To correct the error, complete the following substeps:
  - a. Choose **View** → **Upgrade Log** and search the upgrade log to determine where the error occurred.
  - b. Close the error log in the right panel and click the node in the left panel where the error occurred.
  - c. If the error can be fixed without requiring you to restore the version 4.5.1 GCD database (in case of a domain upgrade failure) or the object store database (in case of an object store upgrade failure), fix the condition that caused the error and then click **Reenable Upgrade** next to the failed node to reset the node to the ready state.
  - d. If the error indicates that you need to restore the version 4.5.1 GCD database to its state before the upgrade, click **Reenable Upgrade** at the top of the right panel for each domain node to reset it to the ready state. Use your database tools to restore the database to its state before the upgrade of Content Engine from version 3.5.2.
  - e. If the error indicates that you need to restore the object store database to its state before the upgrade, click **Reenable Upgrade** at the top of the right panel to reset all nodes of the object store to ready state. Use your database tools to restore the database to its state before the upgrade of Content Engine from version 3.5.2. If the error occurred during the Upgrade Addons phase because of classes or properties that were removed from the object store and imported by a System Addon, reimport the Addon XML file to replace the missing classes or properties. Then, log in to version 4.5.1 FP2 of IBM FileNet Enterprise Manager and refresh the object stores node. If the object store that failed is visible, delete it.
  - f. Click **Bring Online** for each object store selected for upgrade that Content Engine Upgrade Tool did not attempt to upgrade (because of the error that stopped processing) if you need the version 3.5.2 object stores available while you are resolving the object store or domain error.
  - g. Return to step 2 on page 312.
4. If the upgrade succeeds, and you have additional object stores to upgrade, return to step 1 on page 312.

**Important:** When you have successfully upgraded an object store, Content Engine Web Upgrade Tool prevents you from trying to upgrade the object store again.

5. When you have upgraded all the object stores, choose **View** → **Upgrade Report** to see a summary of the results of the upgrades.

#### **Upgrading a version 3.5.2 FileNet P8 domain into an existing version 4.5.1 FileNet P8 domain:**

You have an existing version 4.5.1 FileNet P8 domain (which already contains object stores) and are upgrading version 3.5.2 object stores into it.

To upgrade a version 3.5.2 domain into an existing version 4.5.1 FileNet P8 domain:



1. Resolve any conflicts between the GCD objects (such as marking sets and fixed content devices) and object store names in the version 4.5.1 domain with the corresponding GCD objects and object store names in the version 3.5.2 domain.
2. Choose **File** → **Start New Upgrade** to start an upgrade of version 3.5.2.
3. Enter the location of the GCD file `sysinit.dat` on the Windows machine where version 3.5.2 of Content Engine is installed. If you previously copied `sysinit.dat` to another location to ensure that it is accessible from a UNIX Content Engine server, you can specify that location instead. Do not rename the file: otherwise, Content Engine Web Upgrade Tool prompts you for a file named `sysinit.dat`.

**Important:** Do not delete the GCD file on the Windows machine where version 3.5.2 of Content Engine is installed.

4. Verify that a file named `upgrade4512.xml` exists. To find the file, navigate to the directory shown in the working directory entry in the right panel of the Upgrade Information page. Then, navigate within that directory to the `FileNet/upgrader` directory. You might need to edit this file to fix errors that occur during the validation or upgrade phases.
5. Verify that a file named `upgrade_trace-timestamp.log` is in the `FileNet/upgrader/logs` directory. Content Engine Web Upgrade Tool creates this file anew each time you log in, and it moves the file from the previous login to the `FileNet/upgrader/logs/backup` directory. This file records all the validation and upgrade activity.

“Upgrading object stores”

You need to upgrade your object stores before they can be made available for use in version 4.5.1 FP2 (or later) of Content Engine.

“Validating object stores” on page 316

Validation determines whether your object stores and other Content Engine data are ready to be upgraded. You cannot upgrade your object stores until they are successfully validated.

#### *Upgrading object stores:*

You need to upgrade your object stores before they can be made available for use in version 4.5.1 FP2 (or later) of Content Engine.

To upgrade object stores:

1. Select the object stores to be upgrade.

If you want to upgrade object stores individually, select them from the left panel of Content Engine Web Upgrade Tool. If you want to select all the object stores at once, choose **Tools** → **Select All Object Stores**. You can upgrade object stores in any order. In either case, the first set of Content Engine object store that you select for upgrade includes (by default) the GCD, domain add-ons, and fixed content devices.

You can clear your selections by choosing **Tools** → **Clear All Object Stores**. (The **Clear All Object Stores** menu choice is unavailable until you select at least one object store.)

**Tip:** The upgrade log file can get long. For ease in viewing the log, upgrade only one object store at a time.

2. Click **Upgrade**. The right panel displays a log showing the progress of the upgrade.



Each time you click **Upgrade**, Content Engine Web Upgrade Tool creates a file named `upgrade-running.log` in the `FileNet/upgrader/logs` directory, and copies the previous `upgrade-running.log` file to the `upgrader_trace-timestamp.log` file in the `FileNet/upgrader/logs/backup` directory.

After the upgrade starts, you can pause it by clicking **Pause**. The upgrade pauses as soon as it finishes upgrading whatever object store node it is currently processing. To resume the upgrade, click **Resume**.

If you exit the browser in which Content Engine Web Upgrade Tool is running, an upgrade that is in progress continues in the background. If you log back in, you see the upgrade status at its current state in the right panel.

Content Engine Web Upgrade Tool indicates which object store it is upgrading by changing the appearance of the corresponding icon in the left panel. The tool also changes the appearance of each icon to indicate that it has completed the upgrade of an object store.

Content Engine Web Upgrade Tool also puts the most recent upgrade report file `upgrade.htm` into the directory `FileNet/upgrader/reports` and moves the (time-stamped) report file from the previous upgrade into the directory `FileNet/upgrader/reports/backup`. Both directories are relative to the location specified in the working directory on the Upgrade Information page.

3. If Content Engine Web Upgrade Tool detects an error in upgrading an object store, it halts. To correct the error, complete the following substeps:
  - a. Choose **View** → **Upgrade Log** and search the upgrade log to determine where the error occurred.
  - b. Close the error log in the right panel and click the node in the left panel where the error occurred.
  - c. If the error can be fixed without requiring you to restore the version 4.5.1 GCD database (in case of a domain upgrade failure) or the object store database (in case of an object store upgrade failure), fix the condition that caused the error and then click **Reenable Upgrade** next to the failed node to reset the node to the ready state.
  - d. If the error indicates that you need to restore the version 4.5.1 GCD database to its state before the upgrade, click **Reenable Upgrade** at the top of the right panel for each domain node to reset it to the ready state. Use your database tools to restore the database to its state before the upgrade of Content Engine from version 3.5.2.
  - e. If the error indicates that you need to restore the object store database to its state before the upgrade, click **Reenable Upgrade** at the top of the right panel to reset all nodes of the object store to ready state. Use your database tools to restore the database to its state before the upgrade of Content Engine from version 3.5.2. If the error occurred during the Upgrade Addons phase because of classes or properties that were removed from the object store and imported by a System Addon, reimport the Addon XML file to replace the missing classes or properties. Then, log in to version 4.5.1 FP2 of IBM FileNet Enterprise Manager and refresh the object stores node. If the object store that failed is visible, delete it.
  - f. Click **Bring Online** for each object store selected for upgrade that Content Engine Upgrade Tool did not attempt to upgrade (because of the error that stopped processing) if you need the version 3.5.2 object stores available while you are resolving the object store or domain error.
  - g. Return to step 2 on page 314.
4. If the upgrade succeeds, and you have additional object stores to upgrade, return to step 1 on page 314.

**Important:** When you have successfully upgraded an object store, Content Engine Web Upgrade Tool prevents you from trying to upgrade the object store again.

5. When you have upgraded all the object stores, choose **View** → **Upgrade Report** to see a summary of the results of the upgrades.

*Validating object stores:*

Validation determines whether your object stores and other Content Engine data are ready to be upgraded. You cannot upgrade your object stores until they are successfully validated.

To validate object stores:

1. For each fixed content device in the left panel of the Upgrade Information window that needs info (as indicated by its icon in the left panel), select the device and specify the required parameter values in the right panel.

**Important:** The SnapLockPassword parameter value is not stored. If you log off Content Engine Web Upgrade Tool and log back on, you must reenter the value.

2. If Hitachi [SnapLock] or IBM [Tivoli] are listed among the fixed content devices in the left panel, complete the following substeps. Otherwise, Content Engine Web Upgrade Tool does not process them:
  - a. Choose **Tools** → **Edit XML**.
  - b. In the upgrade4512.xml file, replace all occurrences of Unsupported with UpgradeFinished to make Content Engine Web Upgrade Tool ignore these unsupported fixed content devices and fixed file stores (if any) in the object stores you upgrade.
  - c. Click **Save**.
3. Select the object stores to be validated. Initially, all the object stores are selected for validation. You can validate object stores in any order.

If you want to validate object stores individually, select them from the left panel of Content Engine Web Upgrade Tool. If you want to select all the object stores at once, choose **Tools** → **Select All Object Stores**.

You can clear your selections by choosing **Tools** → **Clear All Object Stores**. (The **Clear All Object Stores** menu choice is unavailable until you select at least one object store.)

4. For each object store that you selected to be validated, complete the following substeps:
  - a. In the right panel, specify the required values from your worksheet.
  - b. If the object store uses fixed file stores, set the values for the root directories to their current locations. (The initial values that appear in these fields are from sysinit.dat and are not correct for version 4.5.1 of Content Engine.)
  - c. When you click **Save**, a prompt reminds you to be sure that you chose the correct data sources for the object store. It also reminds you to verify that you can read from and write to the file stores of the object stores from the Content Engine server.
5. Click **Validate** to validate the object stores that you selected.

Each time you click **Validate**, Content Engine Web Upgrade Tool creates the file validation.log in the directory FileNet/upgrader/logs, and moves the (time-stamped) log file from the previous validation (if any) into the directory

- FileNet/upgrader/logs/backup. Both directories are relative to the location specified in the working directory on the Upgrade Information page.
- Validation errors, such as missing or incorrect parameters, open in the right panel and are also written to `validation.log`.
6. Select **View** → **Validation Log** to check the `validation.log` file for errors. The file opens in a scrollable window. Errors are also displayed in the right panel. You can correct some validation errors within the Content Engine Web Upgrade Tool interface; other errors can be corrected only manually or by using another interface, such as IBM FileNet Enterprise Manager.
  7. To correct a validation error within Content Engine Web Upgrade Tool, complete the following substeps:
    - a. If the error indicates unspecified or invalid JDBC or JDBC XA data sources, choose the correct data source or fix the data source at the application server.
    - b. If the error is in the file store path, specify the correct path.
    - c. If the error is in the file store path, ensure that the file store exists, and that Content Engine can read and write to the file store. (Content Engine Web Upgrade Tool checks that the destination directory associated with the file store exists and that the inbound directory is empty.)
    - d. Click **Save**.
    - e. Click **Validate** and return to step 6.
  8. If the validation log indicates an invalid object store state because of pre-upgrade errors (for example, conflicting classes or properties or pending queue items or publishing requests), log on to version 3.5.2 of IBM FileNet Enterprise Manager and fix the error within the Content Engine 3.5.2 domain.
  9. If you successfully validated an object store, you can upgrade it. To validate more object stores, return to step 3 on page 316.

## Upgrading Content Engine data using Content Engine Upgrader tool

Use Content Engine Upgrader tool to upgrade your version 3.5.2 FileNet P8 domain and object stores if you cannot use Content Engine Web Upgrade Tool.

“Preparing the Content Engine Upgrader tool” on page 318

Before using the Content Engine Upgrader tool to update your Content Engine data, you must install the JDBC driver and edit the upgrader batch file.

“Backing up the version 4.5.1 GCD database” on page 319

You need to back up your version 4.5.1 GCD database before you start upgrading Content Engine data so that in case the upgrade fails, you can recover your original system environment.

“Running the Content Engine Upgrader tool by using the graphical user interface” on page 319

You can use the graphical user interface (GUI) version of the Content Engine Upgrader tool to update your object stores. The graphical user interface provides an interactive interface where each upgrade step is tied to the next, and where you can check the accuracy of your upgrade parameters before starting the upgrade.

“Running the Content Engine Upgrader tool by using the command-line interface” on page 325

You can create an XML upgrade status file and run the Content Engine Upgrader tool by using the command-line interface (CLI). The command-line version of the Upgrader tool does not encrypt the passwords or any other

sensitive data. If your site requires compliance with FIPS-140, then use the graphical user interface to preserve password secrecy.

### Preparing the Content Engine Upgrader tool:

Before using the Content Engine Upgrader tool to update your Content Engine data, you must install the JDBC driver and edit the upgrader batch file.

“Installing the JDBC driver for the Upgrader tool”

If you have installed the Content Engine Upgrader tool on a computer that does not have version 4.5.1 of Content Engine Server installed, then you must install the JDBC driver file.

“Editing the upgrader batch file”

You must specify the database JDBC driver file. You can also increase the minimum and maximum JVM heap sizes.

*Installing the JDBC driver for the Upgrader tool:*

If you have installed the Content Engine Upgrader tool on a computer that does not have version 4.5.1 of Content Engine Server installed, then you must install the JDBC driver file.

For example, if you are upgrading and migrating to a UNIX system, you must run the Upgrader tool on a Windows system to upgrade the existing Content Engine data. You can install the Upgrader tool on Windows without installing all the Content Engine components.

1. See the *IBM FileNet P8 Hardware and Software Requirements* for information about the JDBC driver file for the database type that you need for the Global Configuration Data (GCD) or object stores you are upgrading.
2. Depending on your database type, copy the appropriate JDBC driver file to a directory on the system where the Upgrader tool is installed. For example, copy the file to the C:\jars directory.

**Important:** Do not copy the file to the ...WebSphere\AppServer\lib\ext directory.

### Related information

 Product documentation for IBM FileNet P8 Platform

Download the IBM FileNet P8 Hardware and Software Requirements, as well as PDF's of the rest of the IBM FileNet P8 Platform documentation.

*Editing the upgrader batch file:*

You must specify the database JDBC driver file. You can also increase the minimum and maximum JVM heap sizes.

To increase the minimum and maximum JVM heap sizes and specify the JDBC driver file:

1. Open the upgrader batch file `ce_install_path/tools/upgrade/CE451Upgrader.bat` file in a text editor.
2. Optional: You can edit the upgrader batch file to increase the minimum and maximum JVM heap sizes. The recommended minimum heap size (-Xms) is 512 MB, and the recommended maximum JVM heap sizes (-Xmx) is 1024 MB.

**Tip:** If you are upgrading a system that has only a few object stores and custom objects, you can retain the default settings by skipping to 3. The defaults for the minimum and maximum heap sizes are 256 MB and 512 MB.

To edit the JVM sizes:

#### **Graphical user interface**

Change the line immediately after **GUI:** to the following (without carriage returns):

```
java -Xms512m -Xmx1024m -cp "%CLASSPATH%" %JAVA_OPTIONS%
-Dwasp.location=".\\wasp" com.filenet.upgrader.ui.MainFrame
```

#### **Command line interface**

Change the line immediately after **CLI:** to the following (without carriage returns):

```
java -Xms512m -Xmx1024m -cp "%CLASSPATH%" %JAVA_OPTIONS%
-Dwasp.location=".\\wasp" com.filenet.upgrader.ui.UpgradeUtility %*
```

### **3. Specify the database JDBC driver file.**

- a. Uncomment the set **JDBCPATH** command for your database type by removing `rem` from the beginning of the statement line.
- b. Change **YOURDRIVERPATH** to the full path where you installed the appropriate JDBC driver in the procedure “Installing the JDBC driver for the Upgrader tool” on page 318. For example, if **YOURDRIVERPATH** is `C:/jars`, use one of the following commands:

#### **IBM DB2 for Linux, UNIX and Windows**

```
set JDBCPATH=c:/jars/db2jcc.jar;c:/jars/db2jcc_license_cu.jar
```

#### **IBM DB2 for z/OS**

```
set JDBCPATH=c:/jars/db2jcc.jar;c:/jars/db2jcc_license_cu.jar;
c:/jars/db2jcc_license_cisuz.jar
```

#### **Oracle**

```
set JDBCPATH=c:/jars/ojdbc14.jar
```

#### **Microsoft SQL Server**

```
set JDBCPATH=c:/jars/sqljdbc.jar
```

### **Backing up the version 4.5.1 GCD database:**

You need to back up your version 4.5.1 GCD database before you start upgrading Content Engine data so that in case the upgrade fails, you can recover your original system environment.

To back up your version 4.5.1 GCD database:

User your database administration tools to back up the database that contains the GCD.

### **Running the Content Engine Upgrader tool by using the graphical user interface:**

You can use the graphical user interface (GUI) version of the Content Engine Upgrader tool to update your object stores. The graphical user interface provides an interactive interface where each upgrade step is tied to the next, and where you can check the accuracy of your upgrade parameters before starting the upgrade.

“Starting the Content Engine upgrader tool”

You can use the graphical user interface (GUI) version of the Content Engine Upgrader tool to update your object stores.

“Creating a new XML upgrade status file”

You must create an XML upgrade status file to identify the object stores and Content Engine data to upgrade.

“Configuring authentication, fixed content devices, and object store parameters”

You must provide authentication information for the upgraded data and provide information about your fixed content devices (FCDs) and object stores before you can upgrade the Content Engine data.

“Performing the upgrade” on page 323

You must complete the Content Engine upgrade by applying the settings from your XML upgrade status file.

*Starting the Content Engine upgrader tool:*

You can use the graphical user interface (GUI) version of the Content Engine Upgrader tool to update your object stores.

To run the Upgrader tool:

1. Log on to the machine where the Upgrader tool is installed as `ce_upgrader_tool_user`, which is the user who runs the tool.
2. Double-click the icon for `CE450Upgrader.bat` to start the Upgrader tool.

#### **Related information**

 Specify IBM FileNet P8 accounts

See details on required accounts and related permissions.

*Creating a new XML upgrade status file:*

You must create an XML upgrade status file to identify the object stores and Content Engine data to upgrade.

1. If the Begin Upgrade screen is not displayed, select **File** → **New**.
2. Select the **Upgrade type**.
3. If you are upgrading from Content Engine version 3.5, enter the full path to the GCD file `sysinit.dat`. The default location for version 3.5 is `ce_install_path\sysconfig\sysinit`. If needed, click **Browse** to locate the file.
4. Enter the XML Upgrade Status File full path and file name. If needed, click **Browse** to select the location.
5. Click **Begin**.

The XML upgrade status file is created in the location you specified, and the Provide Content Engine Authentication Information screen is displayed.

*Configuring authentication, fixed content devices, and object store parameters:*

You must provide authentication information for the upgraded data and provide information about your fixed content devices (FCDs) and object stores before you can upgrade the Content Engine data.

1. Specify the Content Engine authentication information:
  - a. In the Specify Content Engine Authentication Information screen, specify the following values:
    - GCD Administrator user name



- GCD Administrator password
- The version 4.5.1 FileNet P8 domain name
- The Content Engine Server URL. The default is `http://server_name:port_number/wsi/FNCEWS40MTOM`.

where *server\_name* is the host name of the machine where Content Engine is deployed, and *port\_number* is the port that Content Engine uses.

- b. Click **Test** to verify the authentication information. A confirmation message is displayed.
  - If the Upgrader tool can connect by using the values that you supplied, a success message is displayed. Click **OK** to close the message box.
  - If the connection validation fails, an error message is displayed. Click **OK** to close the message box, and then edit the field values to correct the problem.
- c. Repeat Step a and Step b as needed until the validation test passes.
- d. Click **Next**.

The Upgrader screen is displayed, with the **Upgrade** tab selected. The Upgrade tree in the left pane lists the items selected for upgrade. The status of each item is indicated with a colored ball. The Upgrade key legend at the bottom of the left pane shows the possible status states: Needs Info, Ready, Processing, Done, Failed, or Unsupported. You must supply data for each item that is in Needs Info state before the upgrade can complete.

2. Specify the property values for any fixed content devices that are in Needs Info state.
  - a. In the Upgrader Tree pane, expand **UpgradeItems** → **CommonGCD** → **Fixed Content Devices**. Click the *device name* to select a fixed content device that is in Needs Info state. The properties and values for the fixed content device are displayed in the right pane in the **FCS Settings** tab.
  - b. Enter the values for the fixed content device settings properties. Values with an \* (asterisk) are required values.

**Important:**

- (CFS-IS) Leave the value of the **CSMCache** parameter blank. You can specify a value after the upgrade completes.  
For descriptions of these parameters, see IBM FileNet P8 help topic **System Administration** → **Content Engine Administration** → **FileNet P8 Domain** → **How to...** → **View/modify P8 domain properties** → **Fixed Content Devices (General tab)**.
- For SnapLock fixed devices where Content Engine version 4.5.1 is on UNIX, make sure you have prepared the UNIX NFS mount to the SnapLock device as instructed in “Configuring storage devices for upgrades” on page 279. The SnapLock share must be an NTFS share, must be mountable as an NFS device, requires proper user mapping. The Root Directory Path, SnapLock User Name, and Device Root Directory must reference UNIX information.
- For Centera devices and where Content Engine version 4.5.1 is installed on a UNIX Server, make sure that new Centera shared libraries have been properly installed on the Content Engine version 4.5.1 server as instructed in “Installing or updating EMC Centera SDK library files” on page 269.

- c. Click **Save**.
- d. Repeat Step a through Step c for each fixed content devices that is in Needs Info state.



3. Specify the property values for any object stores that are in Needs Info state.
  - a. In the Upgrader Tree pane, expand **UpgradeItems** → **Object Stores**. Click the *object store name* to select an item that is in Needs Info state.  
 Each object store might have one or more items in Needs Info state. You must supply the required values for the **Database**, **GCDBObjectStore**, **P8CoreObjectStoreAddons**, **FileStores**, **FixedFileStores**, and **DBStorageArea** as needed for each object store. **FileStores**, **FixedFileStores**, and **DBStorageArea** are displayed only for object stores that have these features enabled.
  - b. Specify the database properties for the selected object store.
    - 1) Click **Database**. The **Database Settings** tab opens in the right pane.
    - 2) Specify values for the following properties:
      - **Database user name**
      - **Database password**
      - **Database type**
      - **Database class**

For this database type	Use this value for the database class
IBM DB2 for Linux, UNIX and Windows or DB2 for z/OS	com.ibm.db2.jcc.DB2Driver
Microsoft SQL Server	com.microsoft.sqlserver.jdbc.SQLServerDriver
Oracle	oracle.jdbc.OracleDriver

- **Database URL**

For this database type	Use this value for the database URL
IBM DB2 for Linux, UNIX and Windows or DB2 for z/OS	jdbc:db2://db_hostname:port/database_name. The default port is 50000.
Microsoft SQL Server	jdbc:sqlserver://db_hostname:port . The default port is 1433.
Oracle	jdbc:oracle:thin:@db_hostname:port:Oracle_instance_SID. The default port is 1521.

- 3) Click **Test** to verify the connection to the database. A confirmation message is displayed.
  - If the Upgrader tool can connect by using the values that you supplied, a success message is displayed. Click **OK** to close the message box.
  - If the connection validation fails, an error message is displayed. Click **OK** to close the message box, and then edit the field values to correct the problem. Repeat Step b until the validation test passes.
- c. Specify the Java Naming and Directory Interface (JNDI) properties for the selected object store. Click **GCDBObjectStore** to enter the Java naming and Directory Interface (JNDI) properties for the selected object store. Specify the following values:
  - Local JNDI name (the non-XA value)
  - Global JNDI name (the XA value)
- d. Specify the File store settings for the selected object store. Click **FileStores** to expand the list of file stores.

- 1) Click the **name** of a file store that is in Needs Info state. The **File Store Path** tab opens in the right pane.
  - 2) UNIX only. Set the Root path to its UNIX equivalent. For example, `/opt/CE_35_filestore_mount/FS_One .`
  - 3) Click **Save** if you made any changes.
  - 4) Repeat Step d for each file store.
- e. If an object store is not yet ready to upgrade, clear the check box for that object store. The selected object store must be in Ready state to be upgraded.
  - f. Take all object stores selected to upgrade offline. In the right pane, select the **Description/Online/Offline** tab, and click **Take Offline**.
  - g. Repeat Step 3 as needed until all the object stores are either in Ready state or disabled for the upgrade.

*Performing the upgrade:*

You must complete the Content Engine upgrade by applying the settings from your XML upgrade status file.

In order for an item to be upgraded, the check box for the corresponding node in the Upgrade Tree pane must be selected, and the item must be in Ready state. Each selected check box maps to a yes value for SelectedForUpgrade within the XML upgrade status file for the corresponding item.

When you click **Start** to initiate an upgrade, the icon next to each item in the Upgrade Tree pane changes color as its state changes. The color code for these states is indicated in the Upgrade Key at the bottom of the Upgrade Tree pane. The icon for any item whose upgrade fails turns red.

As the item upgrade proceeds, its corresponding Status value in the XML upgrade status file changes to reflect the current state of the upgrade. The contents of the Log pane also show the upgrade progress.

If you click **Stop**, the upgrade will stop after completing the current step for the item being upgraded. If an error happens during the upgrade, the corresponding node will be in UpgradeFailed state. Before trying to upgrade an item whose previous upgrade attempt failed, perform the following steps:

1. Fix the error in the item before retrying the upgrade.
2. With the item node selected, click **Reset** to reset the Status value of the item to ReadyToUpgrade.

You can also click **Stop** if the log indicates a condition that makes it pointless to try to upgrade any more of the items selected for upgrade.

To upgrade items:

1. In the Upgrade Tree pane, select the check boxes for all the object stores to be upgraded.
2. Click **Start** to initiate the upgrade and wait until the log or the color of the icon indicates that the upgrade is complete.
3. In the Upgrade Tree pane, select any other object stores to be upgraded, and clear the check boxes for all those object stores already upgraded.
4. Click **Start** to initiate the upgrade. A confirmation message is displayed. Click **Yes** to proceed with the upgrade, or click **No** to cancel.

As the upgrade proceeds, the success or failure of each item being upgraded is captured in a viewable report, which you can view in the Report tab. This report is the same as that generated by running the command-line version of the Upgrader tool.

**Important:** (DB2 only) If a Transaction Log Full exception (SQL Error Code -964) occurs during the upgrade, increase the LOGSECOND parameter (the maximum number of secondary log files) for the database and then repeat Step 4 on page 323.

To change LOGSECOND, run the following command:

```
UPDATE DATABASE CONFIGURATION FOR db_name USING LOGSECOND n
```

where *n* is the new value of LOGSECOND.

If you encounter the exception after the log file counts have been doubled, contact your IBM service representative.

5. To view the upgrade report, click the **Report** tab near the top left of the screen. To save the report as an HTML file, click **Save** in the Report pane.
6. To view the log, click the **Log** tab near the top left of the screen. To copy the log data to the clipboard, click **Copy**. To clear the log data, click **Clear**.
7. If the Upgrader tool successfully upgrades every item, continue at Step 8 on page 325. Otherwise, complete the following steps:
  - a. Use the information (exception code and stack trace) in the command-line output or the log4j file to correct the error.
  - b. Select the failed item and click **Reset** on the **Description** tab to change the status of the item from UpgradeFailed to ReadyToUpgrade.
  - c. If the object store add-on upgrade takes longer than 10 minutes and the upgrade fails with exceptions displayed in the upgrade console or log, you must increase your application server timeout settings. Complete the following steps:
    - 1) Increase your application server transaction timeout value. Make a note of your existing values before you make changes. Depending on your hardware, you might increase the timeout value to as much as 6000 seconds.

#### **IBM WebSphere Application Server**

Navigate to **Application Servers** → *servername* → **Container Services** → **Transaction Services**, and increase the values for **Total transaction lifetime timeout** and **Maximum transaction timeout**.

#### **Oracle WebLogic Server**

Increase the value for **Domain** → **Services** → **JTA** → **Timeout Seconds** and the value for **Servers** → **CEServerInstanceName** → **Configuration** → **Tuning** → **Stuck Thread Max Time**. Use the same value for both settings.

#### **JBoss Application Server**

Edit the `jboss-service.xml` file to set the value for `<attribute name="TransactionTimeout">`.

- 2) Restart the application server.
  - 3) Restart the upgrade for the object store add-ons.
  - 4) After the upgrade completes successfully, you can reset the application server timeout settings to the previous values.
- d. Return to Step 1 on page 323.

8. Update the file count and the file bytes parameter values for the database storage areas associated with the upgraded object stores by running the Update Storage Area Statistics function in the Content Consistency Checker tool. For details, see **System Administration** → **Content Engine Administration** → **Content storage** → **Storage area consistency** → **How to...** → **Update storage area statistics**.

### Running the Content Engine Upgrader tool by using the command-line interface:

You can create an XML upgrade status file and run the Content Engine Upgrader tool by using the command-line interface (CLI). The command-line version of the Upgrader tool does not encrypt the passwords or any other sensitive data. If your site requires compliance with FIPS-140, then use the graphical user interface to preserve password secrecy.

If you do not want to include Content Search Engine as part of your Content Engine upgrade, you must unconfigure content-based retrieval (CBR) from the version 3.5 object store by using the version 3.5 Enterprise Manager.

The Upgrader tool gathers data from the Content Engine version 3.5 Global Configuration Data (GCD) and creates an XML upgrade status file that represents the items that can be upgraded.

The XML file contains placeholders, which you must manually edit, for system settings that cannot be derived from the GCD, such as authentication settings. Each placeholder is indicated by the character string ###.

To run the Upgrader tool:

1. Log on to the machine where the Upgrader tool is installed as *ce\_upgrader\_tool\_user*.
  2. Navigate to the *ce\_install\_path\tools\upgrade* directory, which contains the *CE451Upgrader.bat* file.
  3. Record the path *GCD\_Path* to the *GCD sysinit.dat* file on the Content Engine version 3.5 machine.
  4. Designate a path *XML\_Path* for the XML upgrade status file.
  5. Run the following command to create the XML upgrade status file *upgrade.xml*. Do not enter any line breaks. 

```
CE451Upgrader.bat -i"GCD_Path/sysinit.dat" -o"upgrade.xml"
```
1. "Editing the *upgrade.xml* upgrade status file"  
You must the XML upgrade status file to provide information about the items you want to upgrade.
  2. "Performing the upgrade" on page 326  
You can run the Upgrader tool from the command line to upgrade the items that you selected for upgrade in the *upgrade.xml* upgrade status file.

### Related concepts

 [Specifying IBM FileNet P8 accounts for upgrades](#)

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

*Editing the upgrade.xml upgrade status file:*

You must the XML upgrade status file to provide information about the items you want to upgrade.

The upgrade.xml upgrade status file contains placeholders, for system settings that cannot be derived from the Global Configuration Data (GCD), such as authentication settings. Each placeholder is indicated by the character string ###.

To edit the upgrade.xml upgrade status file:

1. Open the upgrade.xml file in a text editor.
2. Replace each occurrence of the string ### with information that is appropriate for your site.
3. Enter any passwords in plain text. The Upgrader tool does not encrypt the passwords or any other sensitive data. If your site requires compliance with FIPS-140, then use the graphical user interface to preserve password secrecy.
4. Set the value for SelectedForUpgrade to yes to upgrade the item. Set the value for SelectedForUpgrade to no for items that you do not want to upgrade now.
5. Set the Status attribute to ReadyToUpgrade for the items that you want to upgrade. An item is upgraded only if the SelectedForUpgrade value is yes and the Status value is ReadyToUpgrade. The following table describes the possible values for the status:

Status Value	Description
NeedsInfo	Additional configuration information is needed. Change this value to ReadyToUpgrade only after you have supplied all the required values for the item.
ReadyToUpgrade	The item will be upgraded if the corresponding SelectedForUpgrade value is set to yes.
UpgradeStarted	The Upgrader tool has started upgrading the item.
UpgradeFinished	The Upgrader tool has successfully upgraded the item.
UpgradeFailed	The Upgrader tool has failed to upgrade the item.
Unsupported	The Device is not supported by the Upgrader tool. This status applies to fixed content devices only.

6. Save your edits. If you have no file stores or fixed content devices (FCDs) that contain full-text (CBR) indexes (Verity collections) to upgrade, then you have finished preparing for the upgrade.
7. Save your changes and close the XML upgrade status file.

*Performing the upgrade:*

You can run the Upgrader tool from the command line to upgrade the items that you selected for upgrade in the upgrade.xml upgrade status file.

Before upgrading an object store, the Upgrader tool takes the object store offline. After upgrading an object store, the Upgrader tool updates the corresponding Status value for the object store in the upgrade.xml upgrade status file.

1. Log on to the machine where the Upgrader tool is installed as ce\_upgrader\_tool\_user.
2. Navigate to the ce\_install\_path\tools\upgrade directory, which contains CE451Upgrader.bat.

3. Optional: To see the available options, run the Upgrader tool from a command line, as follows: `CE451Upgrader -h`
4. Run the Upgrader tool by entering the following command:  
`CE451Upgrader -i upgrade.xml -r`  
 The `-r` flag is optional. If you include it in the command, the tool generates an HTML report.

**Important:** The tool upgrades only the items that have an initial status of `ReadyToUpgrade` and a `SelectedForUpgrading` value of `yes`.

The Upgrader tool sends a status message to the command line and to a `log4j` logging system as it attempts to upgrade each item. If the upgrade for a specific item fails, the Upgrader tool stops.

5. If the upgrade fails for an item, complete the following steps:
  - a. Use the information (exception code and stack trace) in the command-line output or the `log4j` file to correct the error.
  - b. Edit the `upgrade.xml` file to replace any `Status` value of `UpgradeStarted` or `UpgradeFailed` to `ReadyToUpgrade`.
  - c. If the object store add-on upgrade takes longer than 10 minutes and the upgrade fails with exceptions noted in the log, you must increase your application server timeout settings.

Complete the following steps:

- 1) Increase your application server transaction timeout value. Make a note of your existing values before you make changes. Depending on your hardware, you might must increase the timeout value to as much as 6000 seconds.

#### **IBM WebSphere Application Server**

Navigate to **Application Servers** → `servername` → **Container Services** → **Transaction Services**, and increase the values for **Total transaction lifetime timeout** and **Maximum transaction timeout**.

#### **Oracle WebLogic Server**

Increase the value for **Domain** → **Services** → **JTA** → **Timeout Seconds** and the value for **Servers** → **CEServerInstanceName** → **Configuration** → **Tuning** → **Stuck Thread Max Time**. Use the same value for both settings.


#### **JBoss Application Server**

Edit the `jboss-service.xml` file to set the value for `<attribute name="TransactionTimeout">`.

- 2) Restart the application server.
- 3) Restart the upgrade for the object store add-ons.
- 4) After the upgrade completes successfully, you can reset the application server timeout settings to the previous values.
- d. If the failure occurred due to an error after the database upgrade has completed, then restore your database from backup.
6. Update the file count and the file bytes parameter values for the database storage areas associated with the upgraded object stores by running the Update Storage Area Statistics function in the Content Consistency Checker tool. For details, see **System Administration** → **Content Engine Administration** → **Content storage** → **Storage area consistency** → **How to...** → **Update storage area statistics**.



## Related concepts

 Specifying IBM FileNet P8 accounts for upgrades  
For details on accounts and required permissions, see "Accounts for Content Engine upgrade" in *Plan and Prepare Your Environment for IBM FileNet P8*.

## Updating the database storage area parameters

After you have upgraded your object stores, you need to initialize the parameter values for the associated database storage areas.

Having upgraded the object stores, you now need to set the file count and the file bytes parameter values for the associated database storage areas. These values need to match the values for the database storage areas before the object stores were upgraded.

To update the database storage area parameters:

Run the Content Consistency Checker tool to update the file count and the file bytes parameter values for the database storage areas. You update the values by running the Update Storage Area Statistics function in the tool. For details, see **System Administration** → **Content Engine Administration** → **Content storage** → **Storage area consistency** → **How to...** → **Update storage area statistics**.

## Completing Content Search Engine upgrade from 3.5.2

After you upgrade Content Engine data, you must create new content-search index areas in Enterprise Manager. Then you can enable indexing for designated classes and properties and reindex your stored data. The reindexing process creates new Autonomy K2 collections.

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

This procedure covers the minimum setup and configuration steps to get content-based retrieval (CBR) configured and running with Autonomy K2 for an upgrade from 3.5.2. For more detail on content-based retrieval and Content Engine, see the IBM FileNet P8 help topic **System Administration** → **Content Engine Administration** → **Content-based retrieval** → **How to...** → **Configure CBR**.

**Important:** Where machine name variables are required, IP addresses will not validate. In these cases, you must enter the host name for the machine.

To complete the Content Search Engine upgrade from version 3.5.2:

1. Start Enterprise Manager and log on as the Global Configuration Data (GCD) Administrator.
2. Create a Verity Domain Configuration (VDC).
  - a. 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 Enterprise Manager values for this task, filter by **EM: Verity Domain Configuration Tab** in the **Installation or Configuration Program** column.

- b. Right-click **Enterprise Manager [domain]** in the Enterprise Manager tree and select **Properties**.
    - c. Click the **Verity Domain Configuration** tab.



- d. Enter the following K2 Master Administration Server access information:
    - Host Name - the name of the host of the K2 Master Administration Server.
    - Port - the K2 Master Administration Server port. The default port number is 9950.
    - User Domain - the authentication domain in which your K2 services are installed.
    - User Group - K2 Security Group.
    - Verity Username - K2 Security User.
    - Password - the K2 Security User password.
  - e. Click **Create Configuration** to create a Verity Domain Configuration object.
3. Assign a K2 Broker Server:
    - a. Click the **Verity Server** tab.
    - b. From the Brokers AVAILABLE pane, select the broker and click **Add** to move the server to the Brokers Selected pane.
    - c. Click **OK**.

**Important:** You can assign multiple Broker Servers to a K2 Administration Server, primarily for failover. If one Broker Server goes down, then K2 can switch to another. In this configuration, you must ensure that all Search Servers required to access K2 Collections (index areas) are attached to each Broker Server. A given Content Engine server does not call multiple Broker Servers or merge associated search results. See the appropriate steps of the Configuring Content Search Engine task for instructions on how to create Broker Servers and assign Search Servers.

4. To access the Verity Locale Configuration Guide, complete the following substeps.

**Important:** For information about how the K2 product uses locales and about performance and indexing options, review the Verity Locale Configuration Guide in the Autonomy-supplied documentation set.

- a. Open the Autonomy K2 Dashboard and click **Help**.
  - b. Click **Library** (top right of the screen) to access the Autonomy K2 product guides. Each guide is available in HTML or PDF format.
5. To assign a CBR locale to the object store for which you want to enable indexing, complete the following substeps:
    - a. Right-click the object store in the left pane of Enterprise Manager and choose **Properties** from the context menu.
    - b. In the Properties dialog box, click the **CBR** tab.
    - c. Specify one of the following locales (which are installed by default with Autonomy K2 Content Search Engine software) in the CBR Locale box:
      - uni (multi-language and slower indexing)
      - englishv (enhanced word-stemming and faster indexing)
      - english (limited capabilities and fast indexing)

If you click **Set to Default CBR Locale**, the CBR locale is set to *uni*.

- d. Click **Apply** or **OK**.
6. Create an index area for version 4.5.1 Content Search Engine collections:
    - a. 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 Enterprise Manager values for this task, filter by **EM: Create an Index Area** in the **Installation or Configuration Program** column.

- b. In the Enterprise Manager tree view, expand the **Object Stores** container.
- c. Right-click the object store to which you want to add an index area and select **New** → **Index Area**.
- d. Complete the Create an Index Area wizard by using the values from your worksheet.

**Important:** In the wizard, make sure you set the template type to **FileNet\_FileSystem\_PushAPI**.

For more information about creating indexes, see the IBM FileNet P8 help topic **System Administration** → **Content Engine Administration** → **Content-based retrieval** → **How to...** → **Create Verity index area**.

7. Re-enable content-based retrieval for class definitions by activating the CBR Enabled flag for each class:
  - a. Right-click *class\_name* for the class that you want to configure in the Enterprise Manager tree and click **Properties**.
  - b. Select the **CBR Enabled** check box, and click **OK**.
  - c. Click **Yes** to confirm.
8. For each class property for which you want to enable content-based retrieval, complete the following substeps. The properties you enable must include those that you indexed for content-based retrieval in version 3.5.2 of Content Engine. Refer to the list of properties that you generated by SQL query command on each object store during the pre-upgrade phase of upgrading Content Engine.
  - a. Right-click the base class or subclass that contains the property or properties that you want to reindex and click **Properties** from the context menu.
  - b. Click the **Property Definitions** tab.
  - c. Click the string property you want to enable for indexing and then click **Edit**.
  - d. Select the CBR Enabled check box, and then click **OK**.
9. Reindex each class on which you enabled indexing in the preceding two steps by right-clicking the class and choosing one of the following:
  - **All Tasks** → **Index Class for Content Search**.
  - **All Tasks** → **Index Class for Content Search (include subclasses)**.

For details, see the IBM FileNet P8 help topic **System Administration** → **Content Engine Administration** → **Content-based retrieval** → **How to...** → **Reindex**.

10. To monitor the reindexing progress, complete the following substeps:
  - a. Select and right-click the object store node that contains the index areas that are being reindexed.
  - b. Choose **All Tasks** → **Index Jobs Management**.
  - c. Click **Refresh** to monitor the progress. Click **Close** when reindexing is complete, as indicated by the job status <TERMINATED NORMALLY>.

- Because the version 3.5.2 Content Search Engine collections (indexes) are no longer used, you can save hard drive space by deleting the index directories and all subdirectories. For example, `D:\CE_storage\FS_object_store_name\index`.

**Related tasks**

“Determining the CBR-enabled properties in an object store” on page 223  
 For each object store to be upgraded, you must determine the associated classes and properties that are currently enabled for content-based retrieval (CBR). You enable these properties after the upgrade is complete.

## Upgrading Enterprise Manager

If you did not upgrade Enterprise Manager as part of a Content Engine upgrade, you can upgrade Enterprise Manager interactively or silently.

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

**Important:** You must keep one running version of Enterprise Manager version 3.5.2 until after you upgrade the Content Engine data. You must use Enterprise Manager version 3.5.2 to prepare your version 3.5.2 object stores for the Content Engine Upgrader tool.

To upgrade Enterprise Manager:

- 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 **CE Installer** in the **Installation or Configuration Program** column.

- On the machine where you are upgrading Enterprise Manager, log on as a member of the Local Administrators group or the Power Users group.
- Access the Content Engine software package.
- Start the Enterprise Manager installation.


*Table 31. Installation methods*

Installation method	Description
To install interactively	<ol style="list-style-type: none"> <li>Run the following command in the software package:  <code>P8CE-4.5.1-Win.exe</code></li> <li>Complete the installation program by using the values in your installation worksheet.</li> </ol>

Table 31. Installation methods (continued)

Installation method	Description
To install silently	<ol style="list-style-type: none"> <li>1. Open the CE_silent_install.txt file in the software package for editing.</li> <li>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,AdminTools</li> <li>3. Save your edits.</li> <li>4. Run the following command in the software package: P8CE-4.5.1-WIN.EXE -f CE_silent_install.txt -i silent</li> </ol>

### 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*.

## Upgrading from version 4.0.1 or 4.5.0

Upgrading Content Engine and Content Search Engine from version 4.0.1 or 4.5.0 is a multi-step process.

**Important:** Before you start to upgrade the Content Engine software, ensure that you are at the correct version and fix pack level, as indicated in *Plan and Prepare Your Environment for IBM FileNet P8*.

1. “Completing pre-upgrade Content Engine configuration” on page 334  
You must complete several pre-upgrade procedures to prepare the Content Engine for an upgrade from version 4.0.1 or 4.5.0.
2. “Uninstalling Content Engine and Content Search Engine Client Updater (Version 4.0.1 and AIX)” on page 339  
If you are upgrading from Content Engine version 4.0.1 on AIX, where the root user installed Content Engine version 4.0.1 and the user who is performing the upgrade is non-root, then you must uninstall the existing version of the Content Engine and Content Search Engine Client Updater software.
3. “Upgrading Content Engine software from version 4.0.1 or 4.5.0” on page 341  
On UNIX application servers, you will upgrade Content Engine Server and install Configuration Manager. On Windows application servers, you will upgrade or install these components as needed: Content Engine Server, Configuration Manager, .NET Clients (including Enterprise Manager), Content Engine Upgrader, or FileNet Deployment Manager. You can run the upgrade interactively or silently.
4. “Upgrading Enterprise Manager” on page 344  
If you did not upgrade Enterprise Manager as part of a Content Engine upgrade, you can upgrade Enterprise Manager interactively or silently.
5. “Installing Content Engine software updates” on page 345  
You must apply any updates, fix packs, or interim fixes for the Content Engine software that have been released.

6. "Installing the latest Content Search Engine Client files on Content Engine servers" on page 345  
If your environment includes Content Search Engine, you must install the files that Content Engine uses to communicate with Content Search Engine.
7. "Granting directory permissions to the Configuration Manager user" on page 349  
You must grant the file and directory permissions required by *config\_mgr\_user*, which is the user who runs Configuration Manager.
8. "Configuring Content Engine instances upgraded from version 4.0.1 or 4.5.0" on page 350  
You can configure your upgraded Content Engine instances with Configuration Manager. You must upgrade the Content Engine bootstrap properties for the upgraded Content Engine instance. A single Content Engine application instance equates to one deployed application on your application server.
9. "Installing the latest Process Engine client files on Content Engine servers" on page 356  
You must upgrade the Process Engine Client files on all application server machines where Content Engine Server is deployed.
10. "Deploying upgraded Content Engine instances" on page 358  
You must deploy the upgraded Content Engine on the web application server. Deploying makes the Content Engine application available for use.
11. "Installing storage device source files" on page 362  
If your upgraded IBM FileNet P8 system includes Tivoli Storage Manager or EMC Centera devices, you must install files on the Content Engine server.
12. "Completing Content Engine post-deployment steps" on page 372  
You must complete several Content Engine post-deployment steps before you can put an IBM FileNet P8 system into production.
13. "Verifying the Content Engine deployment" on page 374  
You can verify that the Content Engine deployment was successful by accessing the IBM FileNet P8 System Health page.
14. "Checking the automatic upgrade status for Content Engine data" on page 375  
When you deploy the upgraded Content Engine application on the web application server and start the application, the existing Content Engine data upgrade begins. You can check the progress on the upgrade to confirm that all object stores have been upgraded successfully
15. "Installing the latest Content Engine client files on other IBM FileNet P8 servers (for staged upgrades)" on page 376  
When you upgrade Content Engine software, you must also upgrade the associated Content Engine Client files installed on other machines running IBM FileNet P8 components, for example, on Process Engine and Application Engine servers.
16. "Upgrading Content Search Engine software from version 4.0.1 or 4.5.0" on page 377  
If you used the full-text search feature (CBR) in version 4.0.1 or 4.5.0, to upgrade you must export your current K2 server configurations on each machine, install the new version of Content-Search Engine (Autonomy K2) software, and then import your saved configuration.

## Related information

 General requirements for all FileNet P8 Platform systems  
Check to make sure your software is at the correct fix pack level before you upgrade.

## Completing pre-upgrade Content Engine configuration

You must complete several pre-upgrade procedures to prepare the Content Engine for an upgrade from version 4.0.1 or 4.5.0.

1. “Verifying that publishing requests have been completed”  
You must verify that all publishing requests have completed for each object store before you begin the upgrade from version 4.0.1 or 4.5.0.
2. “Updating the Vital Product Data (VPD) script (version 4.0.1 and Solaris only)” on page 335  
Perform the following steps only if Content Engine Server is at version 4.0.1 on a Solaris machine, a non-root user installed the current version of Content Engine Server, and a different non-root user will upgrade Content Engine.
3. “Creating the webSphereDefaultIsolationLevel custom property (WebSphere)” on page 335  
You must create the `webSphereDefaultIsolationLevel` custom property before you begin the upgrade.
4. “Verifying permissions on the Engine-DS.xml file (JBoss only)” on page 336  
You must verify that the `Engine-DS.xml` file has both read and write permissions before you begin the upgrade.
5. “Backing up the database” on page 336  
You must back up the database before you begin the upgrade.
6. “Shutting down CFS Exporter” on page 337  
If your system includes version 4.0.0 or 4.5 of Content Federation Services (CFS), you must shut down the CFS Exporter before upgrading Content Engine.
7. “Preventing name conflicts with reserved words” on page 337  
You must verify that the object store names, custom classes, or custom properties in your current version do not conflict with reserved words before you begin the upgrade from version 4.0.1 or 4.5.0.
8. “Removing the deployed FileNetEngine application” on page 337  
You must remove the existing FileNetEngine application from the web application server to undeploy or uninstall the application EAR file. Removing the existing version ensures a clean deployment of the upgraded version 4.5.1 Content Engine EAR file.
9. “Clearing the web application server cache” on page 338  
You must clear the cache for the web application server to remove data for the Content Engine version 3.5.2 application to prevent conflicts with the upgraded version.
10. “Editing XA data source XML files (Oracle and JBoss 4)” on page 339  
If you are using an Oracle database with JBoss Application Server version 4.0.5 or version 4.2.3, you must edit the data source XML files to set the `<mbean>` attribute to allow successful connection to the database.

### Verifying that publishing requests have been completed

You must verify that all publishing requests have completed for each object store before you begin the upgrade from version 4.0.1 or 4.5.0.

To verify that publishing requests complete:

1. Start Enterprise Manager if it is not already running.
2. Search for publishing requests in the queue by expanding the **Publishing** folder and clicking **Queue**. Then, click **View** → **All requests**.
3. Verify that the queue (right pane) of publishing requests is empty. If the queue is not empty, wait until the publish requests are processed. If any publish requests are in the In Error state, contact your publishing administrator for the appropriate action to take (such as retrying after correcting the error or just deleting the item).
4. In the list view, under the object store icon, right-click the **Search Results** folder, and choose **New Search**.
5. In the Content Engine Query Builder window, click **Select From Table** → **PublishRequest**.
6. Retain the default settings and click **OK**.
7. Click **Yes** at the prompt for a WHERE clause. Any remaining event items in the queue are displayed in the Query Status window.
8. Remove unwanted items from the queue.
  - a. In the list view, under the object store icon, right-click the **Search Results** folder, and choose **New Search**.
  - b. In the Content Engine Query Builder window, click **Select From Table** → **PublishRequest**.
  - c. Select the **Delete objects** check box in the **Actions** tab of the Search window.
  - d. Click **OK**. Click **OK** again to confirm the deletion.
9. Repeat this procedure for each object store in your environment.

### **Updating the Vital Product Data (VPD) script (version 4.0.1 and Solaris only)**

Perform the following steps only if Content Engine Server is at version 4.0.1 on a Solaris machine, a non-root user installed the current version of Content Engine Server, and a different non-root user will upgrade Content Engine.

1. Navigate to the \$HOME/InstallShield//Universal/FileNet/CE/Gen1/\_vpddb/ directory.
2. Create a backup of the vpd.script file and then edit the vpd.script file as follows:
  - a. Change all instances of \$REG\_CE\_LOCATIONS\$ to the same Content Engine Server installation directory. For example, /opt/FileNet/ContentEngine
  - b. Change all the occurrences of \$40Installeruser\$ to the same Content Engine Server installation directory. For example, /opt/FileNet/ContentEngine
  - c. Save your edits.

### **Creating the webSphereDefaultIsolationLevel custom property (WebSphere)**

You must create the webSphereDefaultIsolationLevel custom property before you begin the upgrade.

Perform this procedure only if both of the following conditions apply to your IBM FileNet P8 environment:

- Your application server is IBM WebSphere Application Server.
- Your database type is DB2 for Linux, UNIX and Windows, DB2 for z/OS, or Microsoft SQL Server.



The `webSphereDefaultIsolationLevel` custom property must exist for the Global Configuration Data (GCD) database XA and non-XA data sources and for the object store data sources.

1. Log on to the WebSphere administrative console.
2. Navigate to **Resources** → **JDBC** → **Data sources**.
3. Click the **GCD non-XA data source name**, for example, **FNGCDDS**.
4. In the Configuration tab, click **Custom properties** under **Additional Properties**.
5. Click **New**, and create a property as follows:
  - a. Set the name to `webSphereDefaultIsolationLevel`.
  - b. Set the value to 2.
  - c. Set the type to `java.lang.String`.
  - d. Click **Apply**.
6. Repeat Step 3 for the **GCD XA data source name**, for example, **FNGCDDSXA**.
7. Click the **Object store non-XA data source name**, for example, **FNOS1DS**.
8. In the Configuration tab, click **Custom properties** under **Additional Properties**.
9. Click **New**, and create a property as follows:
  - a. Set the name to `webSphereDefaultIsolationLevel`.
  - b. Set the value to 2.
  - c. Set the type to `java.lang.String`.
  - d. Click **Apply**.
10. Repeat Step 7 for the **Object store XA data source name**, for example, **FNOS1DSXA**.
11. Save your changes to the master configuration.

### Verifying permissions on the Engine-DS.xml file (JBoss only)

You must verify that the `Engine-DS.xml` file has both read and write permissions before you begin the upgrade.

To verify the permissions:

1. Navigate to the directory containing the `Engine-DS.xml` file. The typical location for this file is:

Option	Description
<b>UNIX</b>	<code>/opt/FileNet/ContentEngine/lib</code>
<b>Windows</b>	<code>C:\Program Files\FileNet\ContentEngine\lib</code>

2. Ensure that the `Engine-DS.xml` file has both read and write permissions.

### Backing up the database

You must back up the database before you begin the upgrade.

1. Use your existing database backup solution to back up each of the Content Engine object store databases.
2. Backup the Global Configuration Data GCD database. The default GCD database name is **FNGCDDDB**.
3. Backup the database for each object store in your environment.

## Shutting down CFS Exporter

If your system includes version 4.0.0 or 4.5 of Content Federation Services (CFS), you must shut down the CFS Exporter before upgrading Content Engine.

Leave the CFS Exporter shut down until you upgrade CFS to version 4.5.1. See *IBM FileNet Content Federation Services Installation and Upgrade Guide* for instructions.

## Preventing name conflicts with reserved words

You must verify that the object store names, custom classes, or custom properties in your current version do not conflict with reserved words before you begin the upgrade from version 4.0.1 or 4.5.0.

Verify that your custom classes and properties do not conflict with the reserved words listed in "New Content Engine classes and properties" in *Plan and Prepare Your Environment for IBM FileNet P8* that describes how you must change any custom class or custom property names in your existing object stores that match the reserved names.

### Upgrading from version 4.0.1 to 4.5.1

Upgrades from version 4.0.1 use the automatic upgrade facility, which automatically renames any conflicting class or property symbolic name that it detects during the upgrade. The upgrade facility writes warning messages for each renamed class or property symbolic name to the `p8_server_error.log` file on the application server where Content Engine is deployed. It also writes these messages to the automatic upgrade status web page. If you know of naming conflicts with version 4.5.0 classes or properties, it is a best practice to resolve these conflicts before you upgrade to version 4.5.1 of Content Engine.

### Upgrading from version 4.5.0 to 4.5.1

Upgrades from version 4.5.0 use the automatic upgrade facility, which will not encounter any conflicting class or property symbolic names.

## Related concepts

 [New Content Engine classes and properties](#)

Learn about new reserved names and how to prevent naming conflicts during an upgrade.

## Removing the deployed FileNetEngine application

You must remove the existing FileNetEngine application from the web application server to undeploy or uninstall the application EAR file. Removing the existing version ensures a clean deployment of the upgraded version 4.5.1 Content Engine EAR file.

To remove the deployed FileNetEngine application:

Undeploy or uninstall the Content Engine EAR file.

Option	Description
WebSphere Application Server	Use the administrative console to undeploy the FileNetEngine application, <code>Engine-ws.ear</code> .
Oracle WebLogic Server	Use the administrative console to undeploy the FileNetEngine application, <code>Engine-wl.ear</code> .

Option	Description
<b>JBoss Application Server</b>	<p>For a standard deployment, remove the Engine-jb.ear file from the <i>jboss_install_dir/server/server_name/</i> deploy directory.</p> <p>For a cluster deployment, remove the Engine-jbc.ear file or Engine-jbc.ear from the <i>jboss_install_dir/all/server_name/</i> deploy directory.</p>

## Clearing the web application server cache

You must clear the cache for the web application server to remove data for the Content Engine version 3.5.2 application to prevent conflicts with the upgraded version.

To clear the cache:

Delete the cache files for you web application server.

Option	Description
<b>WebSphere Application Server</b>	<p>Program Files/IBM/WebSphere/AppServer/ profiles/<i>profilename</i>/temp/ <i>profilenameserver1</i>/FileNetEngine/*.*</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• <i>profilename</i> is profile for Content Engine.</li> <li>• <i>server_name</i> is the name of the Content Engine server instance.</li> </ul>
<b>Oracle WebLogic Server</b>	<p>bea/user_projects/domains/<i>mydomain</i>/ servers/AdminServer/tmp/_WL_user/Engine- wl/*.*</p> <p>bea/user_projects/domains/<i>mydomain</i>/ servers/AdminServer/cache/ EJBCompilerCache/*.*</p> <p>Where <i>mydomain</i> is the name of the Content Engine server instance.</p>
<b>JBoss Application Server</b>	<p><i>jboss_install_dir</i>/server/<i>server_name</i>/ tmp/deploy/*.*</p> <p><i>jboss_install_dir</i>/server/<i>server_name</i>/ work/jboss.web/localhost/FileNet/*.*</p> <p><i>jboss_install_dir</i>/server/<i>server_name</i>/ work/jboss.web/localhost/P8CE/*.*</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• <i>jboss_install_dir</i> is the location where JBoss is installed.</li> <li>• <i>server_name</i> is the name of the Content Engine server instance.</li> </ul>

## Editing XA data source XML files (Oracle and JBoss 4)

If you are using an Oracle database with JBoss Application Server version 4.0.5 or version 4.2.3, you must edit the data source XML files to set the <mbean> attribute to allow successful connection to the database.

To set the <mbean> attribute:

1. Remove the <mbean> tag from the Global Configuration Data (GCD) data source XML file, *jboss\_install\_dir/server/myserver/deploy/FNDGCDXA-ds.xml*.
  - a. Open the data source XML file in a text editor.
  - b. Delete the following <mbean> tag:

```
<mbean
code="org.jboss.resource.adapter.jdbc.vendor.OracleXAExceptionFormatter"
name="jboss.jca:service=OracleXAExceptionFormatter">
<depends optional-attribute name="TransactionManagerService">
jboss:service=TransactionManager
</depends>
</mbean>
```
  - c. Save your change.
2. Remove the <mbean> tag from the object store *FNDosnameXA-ds.xml* data source XML files. Ensure that the data source XML files for your object stores do not have the <mbean> tag.
3. Add the <mbean> tag to the *CEMP-mbean-ds.xml* XML file.
  - a. Create an XML file and name it *jboss\_install\_dir/server/myserver/deploy/CEMP-mbean-ds.xml*.
  - b. Add the following text to the XML file. Do not enter any line breaks in the <mbean> tag.

```
<?xml version="1.0" encoding="UTF-8"?>
<datasources>
<mbean
code="org.jboss.resource.adapter.jdbc.vendor.OracleXAExceptionFormatter"
name="jboss.jca:service=OracleXAExceptionFormatter">
<depends optional-attribute-name="TransactionManagerService">
jboss:service=TransactionManager<</depends>
</mbean>
</datasources>
```
  - c. Save the file.

## Uninstalling Content Engine and Content Search Engine Client Updater (Version 4.0.1 and AIX)

If you are upgrading from Content Engine version 4.0.1 on AIX, where the root user installed Content Engine version 4.0.1 and the user who is performing the upgrade is non-root, then you must uninstall the existing version of the Content Engine and Content Search Engine Client Updater software.

You can run the uninstall program interactively or silently.

“Uninstalling Content Engine interactively (version 4.0.1 and AIX)” on page 340  
If you are upgrading from Content Engine version 4.0.1 on AIX, where the root user installed Content Engine version 4.0.1 and the user who is performing the upgrade is non-root, then you must uninstall the existing version of the Content Engine software. You can uninstall the software interactively.

“Uninstalling Content Engine silently (AIX)” on page 340

If you are upgrading from Content Engine version 4.0.1 on AIX, where the root user installed Content Engine version 4.0.1 and the user who is performing the

upgrade is non-root, then you must uninstall the existing version of the Content Engine software. You can uninstall the software silently.

“Uninstalling Content Search Engine Client Updater interactively (version 4.0.1 and AIX)” on page 341

If you are upgrading from Content Engine version 4.0.1 on AIX, where the root user installed Content Engine version 4.0.1 and the user who is performing the upgrade is non-root, then you must uninstall the existing version of the Content Search Engine Client Updater software. You can uninstall the software interactively.

“Uninstalling Content Search Engine Client Updater silently (version 4.0.1 and AIX)” on page 341

If you are upgrading from Content Engine version 4.0.1 on AIX, where the root user installed Content Engine version 4.0.1 and the user who is performing the upgrade is non-root, then you must uninstall the existing version of the Content Search Engine Client Updater software. You can uninstall the software interactively.

### **Uninstalling Content Engine interactively (version 4.0.1 and AIX)**

If you are upgrading from Content Engine version 4.0.1 on AIX, where the root user installed Content Engine version 4.0.1 and the user who is performing the upgrade is non-root, then you must uninstall the existing version of the Content Engine software. You can uninstall the software interactively.

To uninstall the software

1. Log on as *ce\_install\_user*, which is the user who installed the current version of Content Engine, to the server where Content Engine is installed.
2. Shut down the web application server.
3. Navigate to the *\_uninst2* directory in the current version of Content Engine.
4. Run the following command:  
`uninstaller.bin`

The uninstall might take a while to complete.

### **Uninstalling Content Engine silently (AIX)**

If you are upgrading from Content Engine version 4.0.1 on AIX, where the root user installed Content Engine version 4.0.1 and the user who is performing the upgrade is non-root, then you must uninstall the existing version of the Content Engine software. You can uninstall the software silently.

To uninstall the software

1. Log on as *ce\_install\_user*, which is the user who installed the current version of Content Engine, to the server where Content Engine is installed.
2. Shut down the web application server.
3. Navigate to the *\_uninst2* directory in the current version of Content Engine.
4. Edit the sample response file.
  - a. Open the *CE\_silent\_uninstall.txt* sample response file in a text editor.
  - b. Edit the file using the instructions in the file.
  - c. Save your changes.
5. Run the following command:

```
./uninstaller.bin -options path_to_response_file -silent
```

where *path\_to\_response\_file* is the path to the *CE\_silent\_uninstall.txt* that you edited. The uninstall might take a while to complete.

## Uninstalling Content Search Engine Client Updater interactively (version 4.0.1 and AIX)

If you are upgrading from Content Engine version 4.0.1 on AIX, where the root user installed Content Engine version 4.0.1 and the user who is performing the upgrade is non-root, then you must uninstall the existing version of the Content Search Engine Client Updater software. You can uninstall the software interactively.

To uninstall the software

1. Log on as *ce\_install\_user*, which is the user who installed the current version of Content Engine, to the server where Content Engine is installed.
2. Shut down the web application server.
3. Navigate to the *\_uninst2* directory in the current version of Content Engine.
4. Run the following command:

```
uninstaller.bin
```

The uninstall might take a while to complete.

## Uninstalling Content Search Engine Client Updater silently (version 4.0.1 and AIX)

If you are upgrading from Content Engine version 4.0.1 on AIX, where the root user installed Content Engine version 4.0.1 and the user who is performing the upgrade is non-root, then you must uninstall the existing version of the Content Search Engine Client Updater software. You can uninstall the software interactively.

To uninstall the software

1. Log on as *ce\_install\_user*, which is the user who installed the current version of Content Engine, to the server where Content Engine is installed.
2. Shut down the web application server.
3. Navigate to the *\_uninst2* directory in the current version of Content Engine.
4. Edit the sample response file.
  - a. Open the *CE\_silent\_uninstall.txt* sample response file in a text editor.
  - b. Edit the file by using the instructions in the file.
  - c. Save your changes.
5. Run the following command:

```
./uninstaller.bin -options path_to_response_file -silent
```

where *path\_to\_response\_file* is the path to the *CE\_silent\_uninstall.txt* that you edited. The uninstall might take a while to complete.

## Upgrading Content Engine software from version 4.0.1 or 4.5.0

On UNIX application servers, you will upgrade Content Engine Server and install Configuration Manager. On Windows application servers, you will upgrade or install these components as needed: Content Engine Server, Configuration Manager, .NET Clients (including Enterprise Manager), Content Engine Upgrader, or FileNet Deployment Manager. You can run the upgrade interactively or silently.

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

FileNet Deployment Manager is an optional tool that is used to migrate system data from a test environment to a production environment. See the IBM FileNet P8 help topic **Application Deployment → Get Started with FileNet Deployment Manager** for details.

“Upgrading Content Engine software interactively (Windows)”

You can upgrade the Content Engine software interactively. On Windows application servers, you will upgrade or install these components as needed: Content Engine Server, Configuration Manager, .NET Clients (including Enterprise Manager), Content Engine Upgrader, or FileNet Deployment Manager.

“Upgrading Content Engine software interactively (UNIX)”

You can upgrade the Content Engine software interactively. On UNIX application servers, you will upgrade Content Engine Server and Configuration Manager


“Upgrading Content Engine software silently (Windows)” on page 343

You can upgrade the Content Engine software silently. On Windows application servers, you will upgrade or install these components as needed: Content Engine Server, Configuration Manager, .NET Clients (including Enterprise Manager), Content Engine Upgrader, or FileNet Deployment Manager.

“Upgrading Content Engine software silently (UNIX)” on page 344

You can upgrade the Content Engine software silently. On UNIX application servers, you will upgrade Content Engine Server and Configuration Manager.

### 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*.

### Upgrading Content Engine software interactively (Windows)

You can upgrade the Content Engine software interactively. On Windows application servers, you will upgrade or install these components as needed: Content Engine Server, Configuration Manager, .NET Clients (including Enterprise Manager), Content Engine Upgrader, or FileNet Deployment Manager.

You must upgrade the Content Engine components that are in your existing installation, and you can install new components as needed.


To upgrade Content 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 **CE Installer** in the **Installation or Configuration Program** column.

2. Run the following command in the software package: P8CE-4.5.1-WIN.EXE
3. Complete the installation program screens by using the values in your worksheet.
4. When the installation completes, click **Done** and check for errors in the Content Engine `ce_install_path/ce_install_log_4_5_1.txt` error log file, where `ce_install_path` is the location where Content Engine is 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*.

### Upgrading Content Engine software interactively (UNIX)

You can upgrade the Content Engine software interactively. On UNIX application servers, you will upgrade Content Engine Server and Configuration Manager



To upgrade Content 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 **CE Installer** in the **Installation or Configuration Program** column.

2. Run one of the following commands in the software package, depending on your operating system:

Platform	Command
AIX	P8CE-4.5.1-AIX.BIN
HPUX	P8CE-4.5.1-HPUX.BIN
HPUXi	P8CE-4.5.1-HPUXi.BIN
Linux	P8CE-4.5.1-LINUX.BIN
Solaris	P8CE-4.5.1-SOL.BIN
zLinux	P8CE-4.5.1-ZLINUX.BIN

3. Complete the wizard screens by using the values in your worksheet.
4. When the installation completes, click **Done** and check for errors in the Content Engine *ce\_install\_path/ce\_install\_log\_4\_5\_1.txt* error log file, where *ce\_install\_path* is the location where Content Engine is 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*.

### Upgrading Content Engine software silently (Windows)

You can upgrade the Content Engine software silently. On Windows application servers, you will upgrade or install these components as needed: Content Engine Server, Configuration Manager, .NET Clients (including Enterprise Manager), Content Engine Upgrader, or FileNet Deployment Manager.


To upgrade Content 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 **CE Installer** in the **Installation or Configuration Program** column.

2. Edit the *CE\_silent\_install.txt* file by providing the values from your worksheet.
3. Start the installation program silently: `P8CE-4.5.1-WIN.EXE -f CE_silent_install.txt -i silent`
4. When the installation completes, check for errors in the Content Engine error log file *ce\_install\_path/ce\_install\_log\_4\_5\_1.txt*, where *ce\_install\_path* is the location where Content Engine is 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*.

## Upgrading Content Engine software silently (UNIX)

You can upgrade the Content Engine software silently. On UNIX application servers, you will upgrade Content Engine Server and Configuration Manager.

To upgrade Content 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 **CE Installer** in the **Installation or Configuration Program** column.

2. Edit the `CE_silent_install.txt` file by providing the values from your worksheet.
3. Run one of the following commands in the software package, depending on your operating system:

Platform	Command
AIX	<code>P8CE-4.5.1-AIX.BIN -f CE_silent_install.txt -i silent</code>
HPUX	<code>P8CE-4.5.1-HPUX.BIN -f CE_silent_install.txt -i silent</code>
HPUXi	<code>P8CE-4.5.1-HPUXI.BIN -f CE_silent_install.txt -i silent</code>
Linux	<code>P8CE-4.5.1-LINUX.BIN -f CE_silent_install.txt -i silent</code>
Solaris	<code>P8CE-4.5.1-SOL.BIN -f CE_silent_install.txt -i silent</code>
zLinux	<code>P8CE-4.5.1-ZLINUX.BIN -f CE_silent_install.txt -i silent</code>

4. When the installation completes, check for errors in the Content Engine error log file `ce_install_path/ce_install_log_4_5_1.txt`, where `ce_install_path` is the location where Content Engine is 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*.

## Upgrading Enterprise Manager

If you did not upgrade Enterprise Manager as part of a Content Engine upgrade, you can upgrade Enterprise Manager interactively or silently.

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

To upgrade 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 Configuration Manager values, filter by **CE Installer** in the **Installation or Configuration Program** column.

2. On the machine where you are upgrading Enterprise Manager, log on as a member of the Local Administrators group or the Power Users group.

3. Access the Content Engine software package.
4. Start the Enterprise Manager installation.

Table 32. Installation methods

Installation method	Description
To install interactively	<ol style="list-style-type: none"> <li>1. Run the following command in the software package: P8CE-4.5.1-Win.exe</li> <li>2. Complete the installation program by using the values in your installation worksheet.</li> </ol>
To install silently	<ol style="list-style-type: none"> <li>1. Open the CE_silent_install.txt file in the software package for editing.</li> <li>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,AdminTools</li> <li>3. Save your edits.</li> <li>4. Run the following command in the software package: P8CE-4.5.1-WIN.EXE -f CE_silent_install.txt -i silent</li> </ol>

#### 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 Content Engine software updates

You must apply any updates, fix packs, or interim fixes for the Content Engine software that have been released.

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

To install the Content Engine software updates:

Open the readmes for the Content Engine software updates, and perform the installation procedures in the readmes on each Content Engine instance.

## Installing the latest Content Search Engine Client files on Content Engine servers

If your environment includes Content Search Engine, you must install the files that Content Engine uses to communicate with Content Search Engine.

**Important:** With the initial release of Content Engine 4.5.1, the Content Search Engine 4.5.1 client files are included. Therefore, you are not required to manually install these client files on a new Content Engine server. However, if fix packs of these client files become available, install them manually before you use

Configuration Manager to configure and deploy Content Engine. For instructions on how to obtain the latest Content Search Engine Client software updates, access the IBM FileNet P8 Platform support site.

You can manually install Content Search Engine Client files either interactively or silently:

1. "Removing the existing Content Search Engine Client 4.0.1 files from Content Engine Server machines"  
Remove any previously installed Content Search Engine Client 4.0.1 files from each Content Engine Server machine.
2. "Collecting current Content Engine deployment data"  
Content Engine deployment data provides confirmation that installation of Content Search Engine Client files on Content Engine Server machines has succeeded.
3. "Installing Content Engine Search Client files" on page 347  
You can install the Content Search Engine Client files interactively or silently. These files make it possible for the Content Search Engine server component to communicate with the Content Engine server component.

### Removing the existing Content Search Engine Client 4.0.1 files from Content Engine Server machines

Remove any previously installed Content Search Engine Client 4.0.1 files from each Content Engine Server machine.

You must explicitly remove any previously installed version 4.0.1 of the Content Search Engine Client files because version 4.5.1 of the Content Search Engine Client installer does not completely remove them. If you have no version 4.0.1 files, then return to the parent topic and complete the task.

Remove the version 4.0.1 Content Search Engine Client files, as appropriate for your operating system:

Option	Description
UNIX	Navigate to <i>/InstallDevice/FileNet/ContentEngine/_uninst/cse</i> , run <i>./uninstaller.bin</i> , and follow the dialog boxes to remove the files.
Windows	Navigate to <b>Add/Remove Programs</b> and remove the Content Search Engine Client Updater.

### Collecting current Content Engine deployment data

Content Engine deployment data provides confirmation that installation of Content Search Engine Client files on Content Engine Server machines has succeeded.

To collect current Content Engine deployment data:

1. Enter the following address in a Web browser: `http://ce_app_server_machine_name:port/FileNet/Engine` *ce\_app\_server\_machine\_name* is the host name of the application server machine on which you are deploying Content Engine. *port* is one of the default port numbers used by the application server:

Option	Description
Application Server Type	Default Port Number

Option	Description
WebSphere	9080
WebLogic	7001
JBoss	8080

2. Record the following data on the Web page,

Option	Description
Key	Value
Startup Message	Version number of Content Engine
Process Engine	Version number of Process Engine Client files

### Installing Content Engine Search Client files

You can install the Content Search Engine Client files interactively or silently. These files make it possible for the Content Search Engine server component to communicate with the Content Engine server component.

“Installing Content Search Engine Client files interactively”

You can install the Content Search Engine Client files interactively by running the installation program on all application server machines where Content Engine Server is installed.

“Installing Content Search Engine Client files silently” on page 348

You can install the Content Search Engine Client files silently by editing a silent input file and running the installation program from a command line. You must install Content Search Engine Client files on all application server machines where Content Engine Server is installed.

#### Related tasks

“Installing and configuring Content Search Engine” on page 79

This topic explains how to install and configure Content Search Engine.

#### Installing Content Search Engine Client files interactively:

You can install the Content Search Engine Client files interactively by running the installation program on all application server machines where Content Engine Server is installed.

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

To install Content Search Engine Client 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 Content Search Engine Client values, filter by **CSE Client Installer** in the **Installation or Configuration Program** column.


2. To download the latest software updates, and to determine which of these updates may be required for use with other components and expansion products, contact your service representative.
3. On the machine where Content Engine is to be deployed, log on as *ce\_install\_user*.

4. Locate the Content Search Engine Client installation software. It must be the same version as your Content Search Engine Server software. You must install Content Search Engine and Content Engine software on the same operating system. For example, if Content Engine runs on Windows, locate the Content Search Engine Client installation software that runs on Windows.
5. Start the installation program:

Operating System	Install Program
AIX	P8CSE-CLIENT-4.5.1-AIX.BIN
HP-UX	P8CSE-CLIENT-4.5.1-HPUX.BIN
HP-UXi	P8CSE-CLIENT-4.5.1-HPUXi.BIN
Linux	P8CSE-CLIENT-4.5.1-LINUX.BIN
Linux on System z	P8CSE-CLIENT-4.5.1-ZLINUX.BIN
Solaris	P8CSE-CLIENT-4.5.1-SOL.BIN
Windows	P8CSE-CLIENT-4.5.1-WIN.EXE

6. Complete the Content Search Engine Client installation screens by using the values in your worksheet.
7. Review the following Content Search Engine Client log files:
  - Windows - `cse_client_install_path\CSEClient_install_log_4.5.1.0.log`
  - UNIX - `cse_client_install_path/CSEClient_install_log_4.5.1.0.log`

#### 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 Content Search Engine Client files silently:

You can install the Content Search Engine Client files silently by editing a silent input file and running the installation program from a command line. You must install Content Search Engine Client files on all application server machines where Content Engine Server is installed.

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

To install Content Search Engine Client 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 Content Search Engine Client values, filter by **CSE Client Installer** in the **Installation or Configuration Program** column.

2. To download the latest software updates, and to determine which of these updates might be required with other components and expansion products, contact your service representative.
3. On the machine where Content Engine is to be deployed, log on as `ce_install_user`.
4. Locate the Content Search Engine Client installation software. It must be the same version as your Content Search Engine Server software. You must install Content Search Engine and Content Engine software on the same operating

system. For example, if Content Engine runs on Windows, locate the Content Search Engine Client installation software that runs on Windows.

- Find the `CSE_silent_install.txt` file within the directory that contains the Content Search Engine Client installation software. Then edit the file to specify the location where you want to install the Content Search Engine Client files.

The default installation paths are as follows:

**UNIX** `/opt/IBM/FileNet/ContentEngine/CSEClient`

**Windows**


`C:\Program Files\IBM\FileNet\ContentEngine\CSEClient`

- Start the silent installation of Content Search Engine Client files by running the following command.

Operating System	Install Program
AIX	P8CSE-CLIENT-4.5.1-AIX.BIN -f CSEClient_silent_install.txt -i silent
HP-UX	P8CSE-CLIENT-4.5.1-HPUX.BIN -f CSEClient_silent_install.txt -i silent
HP-UXi	P8CSE-CLIENT-4.5.1-HPUXi.BIN -f CSEClient_silent_install.txt -i silent
Linux	P8CSE-CLIENT-4.5.1-LINUX.BIN -f CSEClient_silent_install.txt -i silent
Linux on System z	P8CSE-CLIENT-4.5.1-ZLINUX.BIN -f CSEClient_silent_install.txt -i silent
Solaris	P8CSE-CLIENT-4.5.1-SOL.BIN -f CSEClient_silent_install.txt -i silent
Windows	P8CSE-CLIENT-4.5.1-WIN.EXE -f CSEClient_silent_install.txt -i silent

- Review the following Content Search Engine Client log files:
  - Windows - `cse_client_install_path\CSEClient_install_log_4.5.1.0.log`
  - UNIX - `cse_client_install_path/CSEClient_install_log_4.5.1.0.log`

**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*.

## Granting directory permissions to the Configuration Manager user

You must grant the file and directory permissions required by `config_mgr_user`, which is the user who runs Configuration Manager.

To grant permissions to the Configuration Manager user:

- Log on as `ce_install_user` to the server where you installed Content Engine.
- Grant permissions to the `config_mgr_user` user for the executable file that you intend to use:

Option	Description
UNIX - graphical user interface	Grant execute permission to configmgr
UNIX - command line	Grant execute permission to configmgr_cl



Option	Description
Windows - graphical user interface	Grant read and execute permission to configmgr.exe
Windows - command line	Grant read and execute permission to configmgr_cl.exe

- 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.
- Log off the Content Engine server and log on again as *config\_mgr\_user*.

## Configuring Content Engine instances upgraded from version 4.0.1 or 4.5.0

You can configure your upgraded Content Engine instances with Configuration Manager. You must upgrade the Content Engine bootstrap properties for the upgraded Content Engine instance. A single Content 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 Engine application environment, then you apply the settings by running the configuration tasks, and then you 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.

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

- (WebSphere Application Server only) For best results, configure no more than one Content Engine instance in a WebSphere profile.
- If you need an accessible software version of Configuration Manager for people with disabilities, use the command-line version of Configuration Manager.
- If your system is HP-RISC, use the command-line version of Configuration Manager.
- If your system is Novell SUSE Linux Enterprise 9, use the command-line version of Configuration Manager.
- 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 complete the tasks on the initial server, you copy the EAR file with the bootstrap settings to the additional servers.

“Configuring upgraded instances by using the graphical user interface”  
You can configure a Content Engine instance by using the graphical user interface version of Configuration Manager.

“Configuring upgraded instances by using the command line” on page 354  
You can configure an upgraded Content Engine instance on a web application server by using the command-line version of Configuration Manager.

### Configuring upgraded instances by using the graphical user interface

You can configure a Content Engine instance by using the graphical user interface version of Configuration Manager.

See the appendix “Configuration Manager user interface reference” on page 538 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.

1. “Starting the Configuration Manager graphical user interface”  
You can start the graphical interface version of Configuration Manager to configure a Content Engine application instance on a web application server.
2. “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.
3. “Creating an upgrade configuration profile” on page 352  
To upgrade Content Engine Server, you must use Configuration Manager to create an upgrade configuration profile. The profile contains deployment, authentication, and database-connection information.
4. “Configuring the upgraded Content Engine instance” on page 353  
You must provide the bootstrap property values to upgrade Content Engine.

#### Starting the Configuration Manager graphical user interface:

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

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 Engine:

Option	Description
UNIX	Run this command: <code>ce_install_path/tools/configure/configmgr</code>
Windows	Perform one of the following actions: <ul style="list-style-type: none"> <li>• Double-click the <b>FileNet Configuration Manager</b> desktop shortcut.</li> <li>• Click <b>Start</b> → <b>All Programs</b> → <b>IBM FileNet P8 Platform</b> → <b>FileNet Configuration Manager</b>.</li> <li>• Run the following command: <code>ce_install_path\tools\configure\configmgr.exe</code></li> </ul>

- 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, you must specify any passwords required by the tasks and for the application server properties before you run the tasks; otherwise, the tasks won't 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 <b>Save all passwords to file when saving a task or profile</b> check box.
To prevent writing passwords to file	Clear the <b>Save all passwords to file when saving a task or profile</b> check box.

3. Click **OK**.

### Creating an upgrade configuration profile:

To upgrade Content Engine Server, you must use Configuration Manager to create an upgrade configuration profile. The profile contains deployment, authentication, and database-connection information.

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 Configuration Manager values, filter by **CM: Create Upgrade Profile** in the Installation or Configuration Program column.

2. Start the Create Upgrade Configuration Profile wizard by using one of the following methods:
  - Select **File** → **New Upgrade Profile**.
  - Click the **Create a profile for an upgrade installation** icon in the toolbar.
3. Complete the configuration screens by referring to the values in your worksheet.
4. The wizard screens that are displayed depend on whether an existing `Servers.xml` file was found in the `ce_install_path\ContentEngine` directory, where `ce_install_path` is the location where Content Engine is installed.

Option	Description
<b>Servers.xml contains 1 server</b>	The upgrade wizard reads the server information from the Servers.xml file. You must name the profile and provide a location for the profile. If the Servers.xml file does not contain information on the deployment type, you must select a deployment type. The wizard creates a profile with the Configure Bootstrap Properties task and the Deploy Application task.
<b>Servers.xml contains more than 1 server</b>	The upgrade wizard reads the server information from the Servers.xml file. You must select a single server to upgrade from the list of servers that was found in Servers.xml. You must name the profile and provide a location for the profile. If the Servers.xml file does not contain information on the deployment type, you must select a deployment type. The wizard creates a profile for the server that you selected with the Configure Bootstrap Properties task and the Deploy Application task.
<b>Servers.xml was not found</b>	The upgrade wizard cannot determine any information about your existing server. You must name the profile, provide a location for the profile, and provide the application server properties. The wizard creates a profile with the Configure Bootstrap Properties task and the Deploy Application task.

- The upgrade profile is displayed as an icon in the left pane with icons for the Configure Bootstrap and Deploy Application tasks.

#### 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 upgraded Content Engine instance:

You must provide the bootstrap property values to upgrade Content Engine.

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


- 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: Upgrade Bootstrap** in the Installation or Configuration Program column.

- With your upgrade profile open, right-click **Configure Bootstrap Properties** in the profile pane, and select **Edit Selected Task**.
- In the **Bootstrap operation** field, select **Upgrade**.

4. In the **Bootstrapped EAR file location** field, enter the fully qualified path to the currently deployed Content Engine EAR file.
5. Select **File** → **Save** to save your changes.
6. Apply the bootstrap property settings by right-clicking **Configure Bootstrap Properties** 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.

### 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 upgraded instances by using the command line

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

Ensure that you have the required accounts and appropriate permissions before you begin.

To configure the upgraded Content Engine instance:

1. Log on to the machine where Content Engine is installed as *config\_mgr\_user*, which is the Configuration Manager user.
2. Change the current directory to *ce\_install\_path/tools/configure*, where *ce\_install\_path* is the path where you installed Content Engine.

As an example, *ce\_install\_path* might be */opt/FileNet/ContentEngine*.

3. At a command prompt, run the **generateupgrade** command to generate the upgrade profile. Enter the command on one line without line breaks.

```
configmgr_cl generateupgrade [-appserver app_server_type] -server server_name
[-deploy deploy_type] -profile myprofile [-silent] [-force] [-help]
```

Where:

#### **-appserver** *appserver\_type*

The **-appserver** *appserver\_type* parameter is required only if the *ce\_install\_path/Servers.xml* file does not exist or does not contain any servers. This parameter specifies the type of application server and must be one of the following values: WebSphere, WebLogic, or JBoss.

#### **-server** *server\_name*

The **-server** *server\_name* parameter indicates the server to create the upgrade profile for. Use the **listservers** command to display a list of valid *server\_name* values before you run the **generateupgrade** command.

#### **-deploy** *deploy\_type*

The **-deploy** *deploy\_type* parameter is required only if the *ce\_install\_path/Servers.xml* file does not exist or does not contain the deployment type for the selected server. This parameter specifies the type of Content Engine deployment. If a value for the deployment type exists in the *Servers.xml* file for the selected server, then the value from the *Servers.xml* file is used instead the value you specify on the command line.

Select one of the following values: *standard*, *cluster*, or *netdeploy* (network deployment).

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

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

#### **-help**

The **-help** parameter is optional and displays a brief message on the command syntax instead of running the command.

The `upgrade.xml` file and one directory named for each existing Content Engine instance is created in the profile directory.

**Important:** If the `generateupgrade` command returns a message saying that an upgrade profile already exists, skip to 4.

4. (IBM WebSphere Application Server or Oracle WebLogic Server only) Set the application server administrator properties:
  - a. Navigate to the `myprofile/mycontent_engine_instance` directory.
  - b. Open the `applicationserver.xml` file in a text editor.

- c. Set the value for the `ApplicationServerAdminUsername` property.
 

```
<propertyname="ApplicationServerAdminUsername">
 <value>administrator_user_name </value>
</property>
```
  - d. Save your changes and close the file.
  - e. Run the **storepasswords** command, which prompts you (respond with yes or no) to choose whether to encrypt and store the web application server administrator password to the `applicationserver.xml` file. If you choose to not save the password, you will need to edit `applicationserver.xml` by specifying the clear text of the password for the `ApplicationServerAdminPassword` property.
 

```
configmgr_cl storepasswords -profile myprofile
```
  - f. Repeat this step as needed to edit the application server properties for each Content Engine instance directory that was created.
5. At a command prompt, run the **execute** command.
 

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

Status messages are displayed in the console.

6. Optional: At a command prompt, check the completion status of the task by running the **checkStatus** command.
 

```
configmgr checkStatus -task configurebootstrap -profile myprofile
```

#### Related concepts

“Configuration Manager command-line reference” on page 555

Configuration Manager can be run from a command line. This section covers the syntax for the command-line version of Configuration Manager.

 [Specifying IBM FileNet P8 accounts for upgrades](#)

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

## Installing the latest Process Engine client files on Content Engine servers

You must upgrade the Process Engine Client files on all application server machines where Content Engine Server is deployed.

“Upgrading the latest Process Engine client files on Content Engine servers interactively”

The upgrade wizard provides an interactive way to upgrade the Process Engine Client files. You can use the values you collected on your worksheet to fill in the required value for each field on the wizard screens.

“Upgrading the latest Process Engine client files on Content Engine servers silently” on page 357

You can upgrade the Process Engine Client software on the Content Engine server by using a silent input text file and running the upgrade program from the command line. Use the values in your installation and upgrade worksheet to edit the silent input text file before you run the upgrade.

### Upgrading the latest Process Engine client files on Content Engine servers interactively

The upgrade wizard provides an interactive way to upgrade the Process Engine Client files. You can use the values you collected on your worksheet to fill in the required value for each field on the wizard screens.



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

To upgrade the Process Engine Client 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 Content Engine values, filter by **PE Client Installer** in the **Installation or Configuration Program** column.

2. To download the latest software updates, and to determine which of these updates might be required for use with other components and expansion products, contact your service representative.
3. On the machine where Content Engine is to be deployed, log on as *ce\_upgrade\_user*.
4. Access the Process Engine Client install software from the Process Engine installation software. The version of the install software must match the version of Process Engine.
5. Expand the (TAR or ZIP) Process Engine Client install software.
6. Shut down all instances of Enterprise Manager and any other Content Engine client applications, such as Application Engine.
7. Run the command for the installation program according to your operating system.

Operating System	Install Program
AIX	P8PE-CLIENT-4.5.1-AIX.BIN
HPUX	P8PE-CLIENT-4.5.1-HPUX.BIN
HPUXi	P8PE-CLIENT-4.5.1-HPUXI.BIN
Linux	P8PE-CLIENT-4.5.1-LINUX.BIN
Solaris	P8PE-CLIENT-4.5.1-SOL.BIN
Windows	P8PE-CLIENT-4.5.1-WIN.EXE
zLinux	P8PE-CLIENT-4.5.1-ZLINUX.BIN

8. Complete the Process Engine client install screens.

### 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*.

### Upgrading the latest Process Engine client files on Content Engine servers silently

You can upgrade the Process Engine Client software on the Content Engine server by using a silent input text file and running the upgrade program from the command line. Use the values in your installation and upgrade worksheet to edit the silent input text file before you run the upgrade.

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

To install the Process Engine Client files 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 **PE Client Installer** in the **Installation or Configuration Program** column.

2. To download the latest software updates, and to determine which of these updates might be required for use with other components and expansion products, contact your service representative.
3. On the machine where Content Engine is to be deployed, log on as *ce\_upgrade\_user*.
4. Access the Process Engine Client install software from the Process Engine installation software. The version of the install software must match the version of Process Engine.
5. Expand the (TAR or ZIP) Process Engine Client install software.
6. Shut down all instances of Enterprise Manager and any other Content Engine client applications, such as Application Engine.
7. In the expanded install software, open the file PEClient\_silent\_install.txt and edit it as follows: Change the Variable\_CheckboxCE line to the following line:
 

```
-V Variable_CheckboxCE="true"
```
8. Save your edits.
9. Run one of the commands in the following table to perform the silent install:

Operating System	Install Program
AIX	P8PE-CLIENT-4.5.1-AIX.BIN -silent -options "PEClient_silent_install.txt"
HPUX	P8PE-CLIENT-4.5.1-HPUX.BIN -silent -options "PEClient_silent_install.txt"
HPUXi	P8PE-CLIENT-4.5.1-HPUXI.BIN -silent -options "PEClient_silent_install.txt"
Linux	P8PE-CLIENT-4.5.1-LINUX.BIN -silent -options "PEClient_silent_install.txt"
Solaris	P8PE-CLIENT-4.5.1-SOL.BIN -silent -options "PEClient_silent_install.txt"
Windows	P8PE-CLIENT-4.5.1-WIN.EXE -silent -options "PEClient_silent_install.txt"
Linux on System z	P8PE-CLIENT-4.5.1-ZLINUX.BIN -silent -options "PEClient_silent_install.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*.

## Deploying upgraded Content Engine instances

You must deploy the upgraded Content Engine on the web application server. Deploying makes the Content Engine application available for use.

**Restriction:** Use the command-line version of Configuration Manager if any of these conditions is true:

- Your system is HP-RISC. You can configure Content Engine only with the command line.

- Your system is Novell SUSE Linux Enterprise 9. You can configure Content Engine only with the command line.
- You need an accessible software version of Configuration Manager for people with disabilities to use.
  - “Deploying upgraded instances by using the graphical user interface”  
You can deploy an upgraded Content Engine instance on the web application server by using the graphical user interface version of Configuration Manager. Deploying makes the Content Engine application available for use.
  - “Deploying upgraded instances by using the command line” on page 360  
You can deploy an upgraded Content Engine instance on a web application server by using the command-line version of Configuration Manager. Deploying makes the Content Engine application available for use.

### Deploying upgraded instances by using the graphical user interface

You can deploy an upgraded Content Engine instance on the web application server by using the graphical user interface version of Configuration Manager. Deploying makes the Content Engine application available for use.

Make sure that the application server is running or stopped, depending on its type:

Table 33. Required Application Server State

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

For more information about 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. See the appendix “Configuration Manager user interface reference” on page 538 for complete information about using the graphical user interface.

To deploy Content 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 values, filter by **CM: Deploy Application** in the Installation or Configuration Program column. For general information about the worksheet file, such as filtering details, see “Using the installation and upgrade worksheet” in *Plan and Prepare Your Environment for IBM FileNet P8*.


2. Log on to the application server machine as *config\_mgr\_user*, the Configuration Manager user.
3. Start Configuration Manager by running one of the following commands, depending on the operating system that runs on the machine where you installed Content Engine:

Option	Description
UNIX	<code>ce_install_path/tools/configure/configmgr</code>
Windows	Perform one of the following actions: <ul style="list-style-type: none"> <li>• Double-click the <b>FileNet Configuration Manager</b> desktop shortcut.</li> <li>• Select <b>Start</b> → <b>All Programs</b> → <b>IBM FileNet P8 Platform</b> → <b>FileNet Configuration Manager</b>.</li> <li>• Run <code>ce_install_path\tools\configure\configmgr.exe</code>.</li> </ul>

4. If you upgraded your application server and then redeployed Content Engine before upgrading Content Engine, click the **Edit Application Server Properties** icon and correct any obsolete parameter values for your application server type.
5. Select **File** → **Open Configuration Profile**, and use the information in your worksheet to specify the values for the parameters in the wizard screens.
6. In the Open Configuration Profile wizard, enter the path to the profile for the Content Engine instance, and then click **Finish**.
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. Select **File** → **Save**.
10. Enable the task. By default, the **Deploy Application** task is disabled. 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.
11. Right-click the **Deploy Application** task in the left pane, and select **Run Task**. Running the deploy task can take a few minutes. The task execution status messages are displayed in the Console pane below the deploy application properties.
12. Repeat this procedure as needed for each Content Engine instance.

#### Related concepts

 [Specifying IBM FileNet P8 accounts for upgrades](#)  
 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*.

#### Deploying upgraded instances by using the command line

You can deploy an upgraded Content Engine instance on a web application server by using the command-line version of Configuration Manager. Deploying makes the Content Engine application available for use.

Ensure that the application server is running or stopped:

Table 34. Required Application Server State

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

See “Configuration Manager command-line reference” on page 555 for syntax details.

To deploy a Content Engine instance from the command line:

1. Log on to the application server machine as the *config\_mgr\_user* user, which is the Configuration Manager user.
2. If you upgraded the version of your application server, or if you moved it to a new directory or device and then redeployed Content Engine before upgrading Content Engine to version 4.5.1 from version 4.0.1 or 4.5.0, perform the following substeps:
  - a. Open the *applicationserver.xml* file for editing.
  - b. Correct any obsolete parameter values for your application server type.
  - c. Save your edits.

3. Set the current directory to *ce\_install\_path/tools/configure*, where *ce\_install\_path* is the path where you installed Content Engine.

4. Run the following command to apply the settings in the *deployapplication.xml* file:

```
configmgr execute -task deployapplication -profile myprofile
```

where 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 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".

5. Optional: Run the following command to check the completion status of the *DeployApplication* task.

```
configmgr checkstatus -task deployapplication -profile myprofile
```

6. Repeat this procedure as needed to deploy any additional Content Engine instances.

## 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 storage device source files

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

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

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 and adding native API library paths (WebLogic)” on page 363

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 and adding native API library paths (JBoss)” on page 366

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 368

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

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

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

1. “Installing Tivoli Storage Manager client”  
Install the Tivoli Storage Manager client software on each application server where Content Engine is deployed.
2. “Copying the Tivoli Storage Manager API libraries to additional servers” on page 363  
If you are running a Content Engine server farm, the Tivoli Storage Manager API libraries must be on each server in the farm.
3. “Creating a shared library definition for Tivoli Storage Manager native API library files” on page 363  
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 Engine is deployed.

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 will need to specify the path as the DSMI directory when you create a Tivoli fixed content device in FileNet Enterprise Manager. If you are installing Tivoli Storage Manager client on multiple UNIX hosts, the installation path must be the same on each host. On AIX, install Tivoli Storage Manager client at `/usr/tivoli/tsm/client/ba/bin`.

### Copying the Tivoli Storage Manager API libraries to additional servers:

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

Copy the entire tsm100 directory structure from the Content 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
UNIX	/opt/IBM/FileNet/ContentEngine/tsm100
Windows	C:\Program Files\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.

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. For the detailed procedure on creating the shared library, visit <http://www.ibm.com/software/webservers/appserv/was/library/>.
  - 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.

### Installing Tivoli Storage Manager client and adding native API library paths (WebLogic)

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

1. "Installing Tivoli Storage Manager client"  
Install the Tivoli Storage Manager client software on each application server where Content Engine is deployed.
2. "Copying the Tivoli Storage Manager API library files to additional servers" on page 364  
If you are running a Content Engine server farm, the Tivoli Storage Manager API libraries must be on each server in the farm.
3. "Creating a shared library definition for Tivoli Storage Manager native API library files" on page 364  
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 Engine is deployed.

1. Download the Tivoli Storage Manager client software from the IBM Support site at <http://www.ibm.com/support/docview.wss?uid=swg24019757>.



- 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 will need to specify the path as the DSMI directory when you create a Tivoli fixed content device in FileNet Enterprise Manager. If you are installing Tivoli Storage Manager client on multiple UNIX hosts, the installation path must be the same on each host. On AIX, install Tivoli Storage Manager client at `/usr/tivoli/tsm/client/ba/bin`.

**Copying the Tivoli Storage Manager API library files to additional servers:**

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

Copy the entire `tsm100` directory structure from the Content 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
UNIX	<code>/opt/IBM/FileNet/ContentEngine/tsm100</code>
Windows	<code>C:\Program Files\IBM\FileNet\ContentEngine\tsm100</code>

**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.

- Open in an edit window the WebLogic script that sets up the domain environment. The following are example paths to this script:

Option	Description
UNIX	<code>/opt/bea/user_projects/domains/base_domain/bin/setDomainEnv.sh</code>
Windows	<code>C:\bea\user_projects\domains\base_domain\bin\setDomainEnv.cmd</code>

- Edit the WebLogic script by adding the lines shown below, for your operating system, just before the line in which the `WL_HOME` variable is set. Substitute your version identifier in place of `weblogic92` as appropriate. There is no carriage return after any line that ends with `/`, `\`, `;`, or `_`.

Option	Description
AIX	<pre>TSMAPILIB=/opt/IBM/FileNet/ContentEngine/tsm100 LIBPATH=\${LIBPATH}:\${TSMAPILIB} EXT_POST_CLASSPATH=\${EXT_POST_CLASSPATH}:\${TSMAPILIB}/TsmJavaApi.jar export LIBPATH EXT_POST_CLASSPATH WL_HOME="/opt/bea/weblogic92" export WL_HOME</pre>

Option	Description
<b>HP-UX (32-bit)</b>	<pre>TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 SHLIB_PATH=\${SHLIB_PATH}:\${TSMAPILIB} EXT_POST_CLASSPATH= \${EXT_POST_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export SHLIB_PATH EXT_POST_CLASSPATH WL_HOME="/opt/bea/weblogic92" export WL_HOME</pre>
<b>HP-UX (64-bit) and HP-UXi</b>	<pre>TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 SHLIB_PATH=\${SHLIB_PATH}:\${TSMAPILIB} EXT_POST_CLASSPATH= \${EXT_POST_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export SHLIB_PATH EXT_POST_CLASSPATH JAVA_OPTIONS="\${JAVA_OPTIONS} -d64" export JAVA_OPTIONS WL_HOME="/opt/bea/weblogic92" export WL_HOME</pre>
<b>Linux</b>	<pre>TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 LD_LIBRARY_PATH=\${LD_LIBRARY_PATH}: \${TSMAPILIB} EXT_POST_CLASSPATH= \${EXT_POST_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export LD_LIBRARY_PATH EXT_POST_CLASSPATH WL_HOME="/opt/bea/weblogic92" export WL_HOME</pre>
<b>Solaris (32-bit)</b>	<pre>TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 TSMCLIENTLIB=/opt/tivoli/tsm/ client/api/bin LD_LIBRARY_PATH=\${LD_LIBRARY_PATH}: \${TSMAPILIB}:\${TSMCLIENTLIB} EXT_POST_CLASSPATH= \${EXT_POST_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export LD_LIBRARY_PATH EXT_POST_CLASSPATH WL_HOME="/opt/bea/weblogic92" export WL_HOME</pre>
<b>Solaris (64-bit)</b>	<pre>TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 TSMCLIENTLIB=/opt/tivoli/tsm/ client/api/bin64 LD_LIBRARY_PATH_64= \${LD_LIBRARY_PATH_64}: \${TSMAPILIB}:\${TSMCLIENTLIB} EXT_POST_CLASSPATH= \${EXT_POST_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export LD_LIBRARY_PATH_64 EXT_POST_CLASSPATH JAVA_OPTIONS="\${JAVA_OPTIONS} -d64" export JAVA_OPTIONS WL_HOME="/opt/bea/weblogic92" export WL_HOME</pre>

Option	Description
Windows	<pre>set TSMAPILIB=C:\Program Files\IBM\ FileNet\ContentEngine\tsm100 set PATH=%PATH%;%TSMAPILIB% set EXT_POST_CLASSPATH=%EXT_POST_ CLASSPATH%;%TSMAPILIB%\TsmJavaApi.jar set WL_HOME=C:\bea\weblogic92</pre>

3. If you are using WebLogic Node Manager to start and stop WebLogic Managed Servers in a clustered environment, you must enable Node Manager to use the appropriate start script:
  - a. Open for editing the node manager configuration file `WL_HOME/common/nodemanager/nodemanager.properties`.
  - b. Set the `StartScriptEnabled` property to `true` (default is `false`).
  - c. Set the `StartScriptName` to match the script name used by Node Manager to start the managed server, depending on your operating system:

Option	Description
UNIX	<code>StartScriptName=startManagedWebLogic.sh</code>
Windows	<code>StartScriptName=startManagedWebLogic.cmd</code>

**Important:** If the managed server is not on the same machine as the WebLogic Administration Server and you have an alternate script matching the name of the Managed Server in the domain `bin` directory, make sure to specify that script name instead of the more generic "startManagedWebLogic" script.

4. Save your edits in `nodemanager.properties` and restart the Node Manager.

### Installing Tivoli Storage Manager client and adding native API library paths (JBoss)

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

1. "Installing Tivoli Storage Manager client"  
Install the Tivoli Storage Manager client software on each application server where Content Engine is deployed.
2. "Copying the Tivoli Storage Manager API libraries to additional servers" on page 367  
If you are running a Content Engine server farm, the Tivoli Storage Manager API libraries must be on each server in the farm.
3. "Creating a shared library definition for Tivoli Storage Manager native API library files" on page 367  
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 Engine is deployed.

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 fixed content device in FileNet

Enterprise Manager. If you are installing Tivoli Storage Manager client on multiple UNIX hosts, the installation path must be the same on each host. On AIX, install Tivoli Storage Manager client at /usr/tivoli/tsm/client/ba/bin.

**Copying the Tivoli Storage Manager API libraries to additional servers:**

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

Copy the entire tsm100 directory structure from the Content 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
UNIX	/opt/IBM/FileNet/ContentEngine/tsm100
Windows	C:\Program Files\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.

1. Open in an edit window the JBoss startup script that sets up the domain environment:

Option	Description
UNIX	run.sh
Windows	run.bat

2. Edit the startup script by adding the following lines at the start of the script:  
There is no carriage return after any line that ends with /, \, :, \_ or ;

Option	Description
AIX	TSMAPILIB=/opt/IBM/FileNet/ContentEngine/tsm100 LIBPATH=\${LIBPATH}:\${TSMAPILIB} JBOSS_CLASSPATH=\${JBOSS_CLASSPATH}:\${TSMAPILIB}/TsmJavaApi.jar export LIBPATH JBOSS_CLASSPATH
HP-UX (32-bit)	TSMAPILIB=/opt/IBM/FileNet/ContentEngine/tsm100 TSMCLIENTLIB=/opt/tivoli/tsm/client/api/bin64SHLIB_PATH=\${SHLIB_PATH}:\${TSMAPILIB}:\${TSMCLIENTLIB} JBOSS_CLASSPATH=\${JBOSS_CLASSPATH}:\${TSMAPILIB}/TsmJavaApi.jar export SHLIB_PATH JBOSS_CLASSPATH

Option	Description
HP-UX (64-bit) and HP-UXi	<pre>TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 TSMCLIENTLIB=/opt/tivoli/tsm/client/ api/bin64 SHLIB_PATH=\${SHLIB_PATH}: \${TSMAPILIB}:\${TSMCLIENTLIB} JBOSS_CLASSPATH=\${JBOSS _CLASSPATH}:\${TSMAPILIB} /TsmJavaApi.jar export SHLIB_PATH JBOSS_CLASSPATH JAVA_OPTS="\${JAVA_OPTS} -d64" export JAVA_OPTS</pre>
Linux	<pre>TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 LD_LIBRARY_PATH=\${LD_LIBRARY_PATH}: \${TSMAPILIB} JBOSS_CLASSPATH=\${JBOSS_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export LD_LIBRARY_PATH JBOSS _CLASSPATH</pre>
Solaris (32-bit)	<pre>TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 TSMCLIENTLIB=/opt/tivoli/tsm/client/ api/bin LD_LIBRARY_PATH=\${LD_LIBRARY_PATH}: \${TSMAPILIB}:\${TSMCLIENTLIB} JBOSS_CLASSPATH=\${JBOSS_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export LD_LIBRARY_PATH JBOSS _CLASSPATH</pre>
Solaris (64-bit)	<pre>TSMAPILIB=/opt/IBM/FileNet/ ContentEngine/tsm100 TSMCLIENTLIB=/opt/tivoli/tsm/client/ api/bin64 LD_LIBRARY_PATH_64=\${LD_LIBRARY _PATH_64}:\${TSMAPILIB}: \${TSMCLIENTLIB}JBOSS _CLASSPATH=\${JBOSS_CLASSPATH}: \${TSMAPILIB}/TsmJavaApi.jar export LD_LIBRARY_PATH_64 JBOSS _CLASSPATHJAVA_OPTS="\${JAVA _OPTS} -d64"export JAVA_OPTS</pre>
Windows	<pre>set TSMAPILIB=C:\Program Files\IBM\ FileNet\ContentEngine\tsm100 set PATH=%PATH%;%TSMAPILIB% set JBOSS_CLASSPATH=%JBOSS _CLASSPATH%;%TSMAPILIB%\ TsmJavaApi.jar</pre>

## Installing or updating EMC Centera SDK library files

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

Update the EMC Centera SDK library files if Centera fixed content devices are in your existing environment or if Centera fixed content devices will be added to your IBM FileNet P8 environment.

1. "Installing EMC Centera SDK version 3.2 library files" on page 369  
EMC Center SDK library files enable access between the IBM FileNet P8 environment and EMC Centera fixed content devices.

2. “Configuring EMC Centera SDK environment variables for version 3.2” on page 370  
You must specify values for the environment variables so that Content Engine can access the EMC Centera SDK library files.

**Installing EMC Centera SDK version 3.2 library files:**

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

1. Log on to the Content Engine Server machine as *ce\_install\_user*.
2. Back up or delete any existing EMC Centera SDK library files, which are located in the Default Destination Installation Location column of the following table:

Operating System	Default Destination Installation Location
AIX	/usr/local/Centera_SDK
Solaris	/opt/Centera_SDK
Windows	C:\Centera_SDK
Linux	/usr/local/Centera_SDK
HP-UX	/opt/Centera_SDK
HP-UXi	/opt/Centera_SDK

3. The Centera directory in the Content Engine software package contains the Centera SDK version 3.2 installation files. As shown in the following table, copy the appropriate directory to a location on the Content Engine Server machine, such as /tmp (UNIX) or C:\Temp (Windows).

Operating System	Directory To Be Copied
AIX, Solaris, Windows	Copy the entire Centera directory
Linux	Depending on your version of gcc, copy one of the following directories: Centera/gcc3.3 Centera/gcc4
HP-UX 11i v1 (11.11)	Copy Centera/11i-v1-11.11
HP-UX 11i v2 (11.23)	Copy Centera/11iv1-11.23

4. On the Content 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 Engine Server machine. On UNIX, the installer script will prompt you for the install directory. On Windows, specify the install directory, such as `C:\Centera_SDK`, on the command line.

Option	Description
UNIX	<code>install.sh</code>
Windows	<code>install.bat C:\Centera_SDK</code>

- The installer script creates both 32-bit and 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.

Operating System	Subdirectories of extracted EMC Centera SDK Directory	Description
AIX, Solaris, and Windows	lib	lib has the native library files that are to be installed.
Linux	../gcc3.3/lib	
	../gcc4/lib	
HP-UX	../11i-v1-11.11/lib	
HP-UXi	../11i-v1-11.13/lib	

### Configuring EMC Centera SDK environment variables for version 3.2:

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

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

Option	Description
UNIX	setCenteraLibPath.sh
Windows	setCenteraLibPath.bat

- Modify the sample setup script as indicated in the following table:

Note that the `CENTERA_LIB_PATH` variable needs to point to the sample script, not just the installation directory that contains the script.

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/SDK3.2.607`

then change the installation path of the AIX script to:

`/usr/local/Centera/SDK3.2.607/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.



Operating System	Script Revisions
AIX	<p>From:</p> <pre>CENTERA_LIB_PATH=/usr/local/Centera_SDK/lib/32 LIBPATH=\$LIBPATH:\$CENTERA_LIB_PATH export LIBPATH</pre> <p>to:</p> <pre>CENTERA_LIB_PATH= install_path /lib/32</pre> <p>or:</p> <pre>CENTERA_LIB_PATH= install_path /lib/64</pre>
Solaris	<p>From:</p> <pre>CENTERA_LIB_PATH=/opt/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>
Linux	<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>

Operating System	Script Revisions
HP-UX HP-UXi	<p>From:</p> <pre>CENTERA_LIB_PATH=/opt/Centera_SDK/lib/32 SHLIB_PATH=\$SHLIB_PATH:\$CENTERA_LIB_PATH export SHLIB_PATH</pre> <p>to:</p> <pre>CENTERA_LIB_PATH=install_path/lib/32 SHLIB_PATH=\$SHLIB_PATH:\$CENTERA_LIB_PATH export SHLIB_PATH</pre> <p>or:</p> <pre>CENTERA_LIB_PATH=install_path/lib/64 SHLIB_PATH=\$SHLIB_PATH:\$CENTERA_LIB_PATH export SHLIB_PATH</pre>
Windows	<p>From:</p> <pre>set CENTERA_LIB_PATH=C:\Centera_SDK\lib\32 set PATH=%PATH%;%CENTERA_LIB_PATH%</pre> <p>to:</p> <pre>set CENTERA_LIB_PATH=install_path \lib\32 set PATH=%PATH%;%CENTERA_LIB_PATH%</pre> <p>or:</p> <pre>set CENTERA_LIB_PATH=install_path \lib\64 set PATH=%PATH%;%CENTERA_LIB_PATH%</pre>

- 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.

Application Server	Startup Script (UNIX)	Startup Script (Windows)
WebSphere	setupCmdLine.sh	setupCmdLine.cmd
WebLogic	setDomainEnv.sh	setDomainEnv.cmd
JBoss	run.sh	run.cmd

- Stop and start the application server.

## Completing Content Engine post-deployment steps

You must complete several Content Engine post-deployment steps before you can put an IBM FileNet P8 system into production.

Perform one of the following post-deployment procedures in this topic, depending on your application server type, and then perform the remaining verification procedures.

When you deploy Content Engine after upgrading from version 4.0.1 or 4.5.0, an upgrader servlet automatically upgrades the Global Configuration Data (GCD) database and the object stores.

“Completing post-deployment steps (WebSphere Application Server)” on page 373

If you are using IBM WebSphere Application Server federated user repositories, you must specify the primary administrative user for the web application server.

“Completing post-deployment steps (Oracle WebLogic Server)”

You must restart the web application server to reinitialize the server cache.

“Completing post-deployment steps (JBoss Application Server and Active Directory)”

You must edit the <login-module> XML element in the login-config.xml file to complete the authentication configuration for the Content Engine application.

## Completing post-deployment steps (WebSphere Application Server)

If you are using IBM WebSphere Application Server federated user repositories, you must specify the primary administrative user for the web application server.

To set the administrative user

1. Log in to the WebSphere administrative console.
2. Navigate to **Security** → **Secure administration, applications, and infrastructure**, and click **Configure**.
3. If you have not already done so, specify a unique user (short name) for the **Primary administrative user name**.

**Important:** This name must exist in one of the realms and must be unique.

4. Specify the **Server user identity**. You can specify **Automatically generated server identity**, or specify a user name that exists in one of the repositories. This name must exist in one of the realms and must be unique.
5. Save your changes to the master configuration.
6. Restart the web application server where Content Engine is deployed, as follows:
  - For a stand-alone server, stop and start the application server.
  - For a network deployment on WebSphere Application Server Network Deployment, stop and start the application server where Content Engine is deployed, including the Deployment Manager and all managed nodes.
  - For a cluster, stop and start the cluster.

## Completing post-deployment steps (Oracle WebLogic Server)

You must restart the web application server to reinitialize the server cache.

Restart the Oracle WebLogic Server where Content Engine is deployed.

- For a stand-alone server, stop and start the application server.
- For a cluster, stop and start the cluster.

## Completing post-deployment steps (JBoss Application Server and Active Directory)

You must edit the <login-module> XML element in the login-config.xml file to complete the authentication configuration for the Content Engine application.

1. Make a backup of JBOSS\_HOME/server/all/conf/login-config.xml file.
2. Open the login-config.xml file for editing.
3. Locate the following line inside the scope of the <login-module> XML element at the beginning of the file:

```
<login-module code="org.jboss.security.auth.spi.LdapExtLoginModule"
 flag="sufficient">
```

4. Add the following line immediately after the <login-module line:

```
<module-option name="java.naming.referral">follow</module-option>
```
5. Save your changes.

6. Start the JBoss web application server.

## Verifying the Content Engine deployment

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

1. Verify the state of Content Engine deployment by browsing to the IBM FileNet P8 System Health page:

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

where:

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

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

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

Table 35. Example FileNet P8 System Health page address

Application Server Type	Web Page Address
IBM WebSphere Application Server	<code>http://server:9080/P8CE/Health</code>
Oracle WebLogic Server	<code>http://server:7001/P8CE/Health</code>
JBoss Application Server	<code>http://server:8080/P8CE/Health</code>

2. Verify that the FileNet P8 System Health page contains the Content 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. In particular, if you are upgrading from version 3.5.2, a red icon appears before the GCD, directory configurations, object stores, storage areas, and sites entries. Also, if you are upgrading from version 3.5.2, no domain name appears yet in the Domain entry.

Table 36. FileNet P8 System Health page contents

Section	Description
<b>Domain</b>	Displays the FileNet P8 domain name if a domain was found.
<b>Global Configuration Database</b>	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.
<b>Directory Configurations</b>	Verifies that at least one directory service is configured and lists the number of configured directory service providers.
<b>PE Connection Points</b>	Displays the number of Process Engine connection points.
<b>PE Isolated Regions</b>	Displays the number of Process Engine isolated regions.
<b>Fixed Content Devices</b>	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.
<b>Object Stores</b>	Verifies that at least one object store exists and lists the number of object stores.
<b>Storage Areas</b>	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.

Table 36. FileNet P8 System Health page contents (continued)

Section	Description
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.

- Optional: Bookmark the FileNet P8 System Health page Web page address in your browser for later use.
- Browse to the FileNet Engine Web page:  
`http://server:port/FileNet/Engine`  
 where:  
*server* is the host name of the machine where Content Engine is deployed.  
*port* is the HTTP port used by the application server where Content Engine is deployed.

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

Table 37. Example FileNet Engine Web page address

Application Server Type	Web Page Address
IBM WebSphere Application Server	<code>http://myserver:9080/FileNet/Engine</code>
Oracle WebLogic Server	<code>http://myserver:7001/FileNet/Engine</code>
JBoss Application Server	<code>http://myserver:8080/FileNet/Engine</code>

- Verify that the FileNet Engine Web page contains the following information:
  - Verify the value in the **Startup Message** key. The Content Engine build and version (for example, `dap451.097`), 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 Engine software is installed.
  - Verify the value in the **Process Engine** key. The Process Engine Client build and version (for example, `pui451.075`), must match the build and version in the `version.txt` file in the TAR or ZIP file of the Process Engine Client installation software.
  - Verify that the values for JDBC driver, server instance, operating system, and other properties match the values that you entered when you configured Content Engine.
- Optional: Bookmark the FileNet Engine Web page in your browser for later use.

## Checking the automatic upgrade status for Content Engine data

When you deploy the upgraded Content Engine application on the web application server and start the application, the existing Content Engine data upgrade begins. You can check the progress on the upgrade to confirm that all object stores have been upgraded successfully

To check the status of the automatic data upgrade:

- Enter the URL for the automatic upgrade status page into your browser.  
`http://server_name:port/FileNet/AutomaticUpgradeStatus`
- Review the status for the FileNet P8 domain or object store.

Table 38. Automatic upgrade status descriptions

Status	Description
Ready	The FileNet P8 domain or object store is ready for use. No automatic upgrade work was performed since the Content Engine server was started.
Completed	<p>The FileNet P8 domain or object store is ready for use. Automatic upgrade work was performed after the Content Engine server was started. Click <b>Completed</b> to view the detailed status for the object store upgrade process.</p> <p>In a multi-server configuration, automatic upgrade work might be in progress on additional servers.</p>
In Progress	<p>The FileNet P8 domain or object store is not available. Automatic upgrade work is currently being performed. The Schema Revision column in the Status for object stores section displays the upgrade phase that was completed. Content Engine version 4.5.1 uses schema revision 15.1.23. Click <b>Completed</b> to view the detailed status for the object store upgrade process.</p>
Not Available	<p>The FileNet P8 domain or object store is not available. The Content Engine server cannot determine the status of the object store. The server is still starting the Content Engine application and cannot access the object store to determine its status, or the object store did not load the object store cache.</p> <p>Wait a while for the server to finish starting. If the server cannot load the object store cache, then the object store cannot be upgraded automatically. The automatic upgrade does not work for upgrades from version 3.5.2 to version 4.5.1.</p>
Asynchronous Upgrade In Progress	<p>Object stores only. The object store is available. Automatic upgrade work was completed and additional asynchronous upgrade work is in progress. The work involves tasks that take a long time to complete, usually due to the large number of documents or custom objects in the object store.</p>

## Installing the latest Content Engine client files on other IBM FileNet P8 servers (for staged upgrades)

When you upgrade Content Engine software, you must also upgrade the associated Content Engine Client files installed on other machines running IBM FileNet P8 components, for example, on Process Engine and Application Engine servers.

In a standard upgrade of your IBM FileNet P8 system, you would install these client files in the course of upgrading each respective component.

However, if you are staging your IBM FileNet P8 upgrade over a period of time and not upgrading one or more of the other IBM FileNet P8 components at this time, you must still perform the Content Engine Client install on the other component machines. In this case, use the following topics in the sections for the other components:

- “Upgrading the Content Engine client files on Process Engine servers” on page 416
- “Installing the latest Content Engine client files on Application Engine servers” on page 449

**Important:**

- You must install the Content Engine client files for any expansion products that use Content Engine Client files, such as:
  - IBM FileNet Workplace XT
  - IBM InfoSphere Enterprise Records
  - IBM FileNet Business Process Framework
- You must redeploy any components that are web-application-server-based, such as Application Engine, Workplace XT, and InfoSphere Enterprise Records, after you upgrade the Content Engine Client files on the associated machines.

## Upgrading Content Search Engine software from version 4.0.1 or 4.5.0

If you used the full-text search feature (CBR) in version 4.0.1 or 4.5.0, to upgrade you must export your current K2 server configurations on each machine, install the new version of Content-Search Engine (Autonomy K2) software, and then import your saved configuration.

1. “Production environment upgrades”

Upgrading of Content Search Engine and related Content Engine data must occur as an in-place upgrade. As such, the data is migrated to 4.5.1 and is no longer usable in the previous version of the IBM FileNet P8 Platform.

2. “Upgrading Content Search Engine” on page 378

Upgrade Content Search Engine on all machines running Autonomy K2 software. Upgrade the K2 Master Administration Server first, before upgrading the K2 Administration Servers.

### Production environment upgrades

Upgrading of Content Search Engine and related Content Engine data must occur as an in-place upgrade. As such, the data is migrated to 4.5.1 and is no longer usable in the previous version of the IBM FileNet P8 Platform.

The index areas are upgraded at the same time as the Content Engine data is upgraded.

To perform an upgrade in a migration scenario, create a duplicate of your IBM FileNet P8 system by performing a backup and then a restore. Using the restored system, complete the migration to 4.5.1. This will leave the original production environment untouched while testing is performed on the new system.



When you're ready to migrate the production environment to the current version, back up the system and then perform the in-place upgrade process on the production environment.

## Upgrading Content Search Engine

Upgrade Content Search Engine on all machines running Autonomy K2 software. Upgrade the K2 Master Administration Server first, before upgrading the K2 Administration Servers.

If you have a multi-server configuration, do not start any K2 services until after all machines have been upgraded.

“Upgrading Content Search Engine software (UNIX)”

To upgrade Content Search Engine, you must upgrade the underlying Autonomy K2 software.

“Upgrading Content Search Engine software (Windows)” on page 384

To upgrade Content Search Engine, you must upgrade the underlying Autonomy K2 software.

“Setting the logon user for the K2 Administration Server service (Windows)” on page 388

To avoid problems when indexing documents using UNC, or viewing UNC-indexed documents, the `k2_os_user` needs to run the K2 Administration Server service.

“Updating the style file of user fields” on page 389

You must edit the Autonomy K2 style file of user fields to add a data field definition for storing the partitioning value of a document.

### Upgrading Content Search Engine software (UNIX):

To upgrade Content Search Engine, you must upgrade the underlying Autonomy K2 software.

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

**Important:** If you have a multiserver configuration, do not start any K2 services until after all Content Search Engine servers have been upgraded. You will need to upgrade the Master Administration Server first.


“Upgrading Content Search Engine interactively (UNIX)”

To upgrade Content Search Engine interactively, you must run an installation program wizard.

“Upgrading Content Search Engine silently (UNIX)” on page 381

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

### 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*.

*Upgrading Content Search Engine interactively (UNIX):*

To upgrade Content Search Engine interactively, you must run an installation program wizard.

An X terminal must be installed on the Content Search Engine server to run the interactive installation program.

To upgrade Content Search 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 Engine values, filter by **CSE Installer** in the **Installation or Configuration Program** column.

2. Access the Autonomy K2 machine and log on as *k2\_os\_user*.
3. To stop the Autonomy K2 Administration Server service and the Tomcat application server, run the following command.

Option	Description
HP-UX	<i>verity_install_path</i> /k2/_hpux/bin/k2adminstop
AIX	<i>verity_install_path</i> /k2/_rs6k43/bin/k2adminstop
Solaris	<i>verity_install_path</i> /k2/_sso126/bin/k2adminstop
Linux	<i>verity_install_path</i> /k2/_ilnx21/bin/k2adminstop

4. Copy the IBM FileNet Content Search Engine installation package to the server.
5. Change directory to the location of the IBM FileNet Content Search Engine installation package.
6. Run the following commands:

```
backup_k2.sh "verity_install_path" "temporary_location_path"
```

where:

*"verity\_install\_path"* is the path to the verity directory in the current installation path.

*"temporary\_location\_path"* is the location in which you want to temporarily back up your Autonomy K2 configuration files, outside of the current installation path, and not used by any other application. Files from this backup are used to restore your existing configuration after you complete the software upgrade.

For example, `backup_k2.sh "/opt/IBM/FileNet/ContentEngine/verity" "/opt/temp"`.

7. If K2 collections are stored anywhere in the installation path, move the *collections directory* and the *temp directory* to a temporary location outside the installation path.
8. Execute the following command to determine which Verity processes are currently running on the machine:

```
ps -eaf | grep k2
```
9. For each Verity process that is running, terminate it by executing the following command:

```
kill -9 pid
```

where *pid* is the process ID.
10. (AIX only) Run the command **slibclean** as the root user to remove all unused libraries from shared memory.

11. Access the IBM FileNet Content Search Engine installation package.
12. Run the installation program.

Platform	Command
AIX	P8CSE-4.5.1.0-AIX.BIN
HPUX	P8CSE-4.5.1.0-HPUX.BIN
Linux	P8CSE-4.5.1.0-LINUX.BIN
Solaris	P8CSE-4.5.1.0-SOL.BIN

13. Complete the installation screens by using the values from your worksheet.
14. Review the following Content Search Engine log files for installation errors. The files are located in the `verity` directory of the installation path.
  - `verity_install_path/verity/cse_install_log_4_5_1.txt`
  - `verity_install_path/verity/vconfig.log`
15. To stop the Autonomy K2 Administration Server service and the Tomcat application server, run the following command.

Option	Description
HP-UX	<code>verity_install_directory/k2/_hpux/bin/k2adminstop</code>
AIX	<code>verity_install_directory/k2/_rs6k43/bin/k2adminstop</code>
Solaris	<code>verity_install_directory/k2/_ssol26/bin/k2adminstop</code>
Linux	<code>verity_install_directory/k2/_ilnx21/bin/k2adminstop</code>

16. Change directory to the location of the IBM FileNet Content Search Engine installation package.
17. To restore your configuration from the backup files, run the following command:

```
restore_k2.sh "temporary_location_path" "verity_install_path"
```

where:

`"temporary_location_path"` is the temporary path you entered earlier in this procedure when you ran the `backup_k2.sh` file.

`"verity_install_path"` is the path to the `verity` directory in the Autonomy K2 installation path.

For example, `restore_k2.bat "/opt/temp" "verity_install_path"`.

18. Add the following lines to the restored file `verity_install_path/data/stylesets/FileNet_FileSystem_PushAPI/style.ufl`:

```
data-table: fce
{
 fixwidth: comp_partition_date 4 unsigned-integer
}
```

**Important:** The purpose of this edit is to enable use of the Content Search Engine partitioning feature, new in version 4.5.1.

19. Run the following commands to set the `setuid` bit for the `vspget` program so that the service runs as root.

**Important:** Most processes for the Autonomy K2 software run as *k2\_os\_user*. However, the *vspget* process must run as root. For details on required accounts and related permissions, see "Specify IBM FileNet P8 accounts" in *Plan and Prepare Your Environment for IBM FileNet P8*.

- `chown root verity_install_path/k2/_platform/bin/vspget`
- `chmod u+s verity_install_path/k2/_platform/bin/vspget`

where *\_platform* is the following directory.


Platform	Directory
HPUX	_hpux
AIX	_rs6k43
Solaris	_ssol26
Linux	_ilnx21

20. If you moved collections earlier in this procedure, restore your *collections directory* and *temp directory* to their original locations.
21. For a single-server configuration, start the K2 services. For multiserver configurations, start the services only after all servers have been upgraded. To start the Verity K2 Administration Server service and the Tomcat service, use the follow command.

Option	Description
HP-UX	<code>nohup verity_install_path/k2/_hpux/bin/k2adminstart</code>
AIX	<code>nohup verity_install_path/k2/_rs6k43/bin/k2adminstart</code>
Solaris	<code>nohup verity_install_path/k2/_ssol26/bin/k2adminstart</code>
Linux	<code>nohup /verity_install_directory/k2/_ilnx21/bin/k2adminstart</code>

22. Access the K2 Dashboard and verify that the services from your previous installation are restored and running.
23. Delete the *temporary\_location\_path* directory of the backup you ran earlier.

### 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*.

*Upgrading Content Search Engine silently (UNIX):*

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

To upgrade Content Search Engine 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 Search Engine values, filter by **CSE Installer** in the **Installation or Configuration Program** column.

2. Access the Autonomy K2 machine and log on as *k2\_os\_user*.
3. To stop the Autonomy K2 Administration Server service and the Tomcat application server, run the following command.

Option	Description
HP-UX	<i>verity_install_path</i> /k2/_hpux/bin/k2adminstop
AIX	<i>verity_install_path</i> /k2/_rs6k43/bin/k2adminstop
Solaris	<i>verity_install_path</i> /k2/_sso126/bin/k2adminstop
Linux	<i>verity_install_path</i> /k2/_ilnx21/bin/k2adminstop

4. Copy the IBM FileNet Content Search Engine installation package to the server.
5. (Master Administration Server only) Change directory to the location of the IBM FileNet Content Search Engine installation package.
6. Run the following commands:  

```
backup_k2.sh "verity_install_path" "temporary_location_path"
```

 where:  
*"verity\_install\_path"* is the path to the verity directory in the current installation path.  
*"temporary\_location\_path"* is where you temporarily back up your Autonomy K2 configuration files, outside of the current installation path.  
*"temporary\_location\_path"* must not and not used by any other application. Files from this backup are used to restore your existing configuration after you complete the software upgrade.  
 For example, `backup_k2.sh "/opt/IBM/FileNet/ContentEngine/verity/k2" "/opt/temp"`.
7. If K2 collections are stored anywhere in the installation path, move the *collections directory* and the *temp directory* to a temporary location outside the installation path.
8. Execute the following command to determine which Verity processes are currently running on the machine:  

```
ps -eaf | grep k2
```
9. For each Verity process that is running, terminate it by executing the following command:  

```
kill -9 pid
```

 where *pid* is the process ID.
10. (AIX only) Run the command **slibclean** as the root user to remove all unused libraries from shared memory.
11. Access the IBM FileNet Content Search Engine installation package.
12. Edit `CSE_silent_install.txt` to reflect the appropriate responses for your installation by using the values in your worksheet. You must install to the same path as your previous installation.
13. Run the following command:  

```
./P8CSE-4.5.1.0-UNIX_type.BIN -f CSE_silent_install.txt -i silent
```
14. Review the following Content Search Engine log files for installation errors. The files are located in the verity directory of the installation path.

- *verity\_install\_path/cse\_install\_log\_4\_5\_1.txt*
- *verity\_install\_path/vconfig.log*

15. To stop the Autonomy K2 Administration Server service and the Tomcat application server, run the following command.

Option	Description
HP-UX	<i>verity_install_path/k2/_hpux/bin/k2adminstop</i>
AIX	<i>verity_install_path/k2/_rs6k43/bin/k2adminstop</i>
Solaris	<i>verity_install_path/k2/_ssol26/bin/k2adminstop</i>
Linux	<i>verity_install_path/k2/_ilnx21/bin/k2adminstop</i>

16. Change directory to the location of the IBM FileNet Content Search Engine installation package.

17. To restore your configuration from the backup files, run the following command:

```
restore_k2.sh "temporary_location_path" "verity_install_path"
```

where:

*"temporary\_location\_path"* is the temporary path you entered earlier in this procedure when you ran the *backup\_k2.sh* file.

*"verity\_install\_path"* is the path to the *verity* directory in the Autonomy K2 installation path.

For example, *restore\_k2.bat "/opt/temp" "/opt/IBM/FileNet/ContentEngine/verity"*.

18. Add the following lines to the restored file *verity\_install\_path/data/stylesets/FileNet\_FileSystem\_PushAPI/style.ufl*:

```
data-table: fce
{
 fixwidth: cemp_partition_date 4 unsigned-integer
}
```

**Important:** The purpose of this edit is to enable use of the Content Search Engine partitioning feature, new in version 4.5.1.

19. Run the following commands to set the *setuid* bit for the *vspget* program so that the service runs as root.

**Important:** Most processes for the Autonomy K2 software run as *k2\_os\_user*. However, the *vspget* process must run as root. For details on required accounts and related permissions, see "Specify IBM FileNet P8 accounts" in *Plan and Prepare Your Environment for IBM FileNet P8*.

```
chown root verity_install_path/k2/_platform/bin/vspget chmod u+s verity_install_path/k2/_platform/bin/vspget
```

where: *\_platform* is the following directory.

Platform	Directory
HPUX	<i>_hpux</i>
AIX	<i>_rs6k43</i>
Solaris	<i>_ssol26</i>


Platform	Directory
Linux	_i1nx21

20. If you moved collections earlier in this procedure, restore your *collections directory* and *temp directory* to their original locations.
21. For a single-server configuration, start the K2 services. For multiserver configurations, start the services only after all servers have been upgraded. To start the Verity K2 Administration Server service and the Tomcat service, use the follow command.

Option	Description
HP-UX	<code>nohup verity_install_path/k2/_hpux/bin/k2adminstart</code>
AIX	<code>nohup verity_install_path/k2/_rs6k43/bin/k2adminstart</code>
Solaris	<code>nohup verity_install_path/k2/_sso126/bin/k2adminstart</code>
Linux	<code>nohup verity_install_path/k2/_i1nx21/bin/k2adminstart</code>

22. Access the K2 Dashboard and verify that the services from your previous installation are restored and running.
23. Delete the *temporary\_location\_path* directory of the backup you ran earlier.

#### 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*.

#### Upgrading Content Search Engine software (Windows):

To upgrade Content Search Engine, you must upgrade the underlying Autonomy K2 software.

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

**Important:** If you have a multiserver configuration, do not start any K2 services until after all Content Search Engine servers have been upgraded. You will need to upgrade the Master Administration Server first.

To upgrade Autonomy K2 Server software on Windows:

“Upgrading Content Search Engine interactively (Windows)” on page 385


To upgrade Content Search Engine interactively, you run a program wizard.

“Upgrading Content Search Engine silently (Windows)” on page 386

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



## 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*.

*Upgrading Content Search Engine interactively (Windows):*

To upgrade Content Search Engine interactively, you run a program wizard.

To upgrade Content Search Engine 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 Search Engine values, filter by **CSE Installer** in the **Installation or Configuration Program** column.

2. Access the Autonomy K2 machine and log on as *k2\_os\_user*.
3. Access Windows Services and stop the two Verity K2 services.
4. Copy the IBM FileNet Content Search Engine installation package to the Autonomy K2 machine.
5. Open a command window and change directory to the location of the IBM FileNet Content Search Engine installation package.
6. Run the following commands:

```
backup_k2.bat "verity_install_path" "temporary_location_path"
```

where:

*"verity\_install\_path"* is the path to the verity directory in the current installation path.

*"temporary\_location\_path"* is the location in which you want to temporarily back up your Autonomy K2 configuration files, outside of the current installation path, and not used by any other application. Files from this backup will be used to restore your existing configuration after you complete the software upgrade.

For example: `backup_k2.bat "C:\Program Files\IBM\FileNet\ContentEngine\verity" "C:\temp"`

7. (Upgrading from version 4.0.1 only) Access the Windows control panel and remove, in reverse order of installation, each Autonomy-related entry that is listed in the Add or Remove Programs control panel. Ensure that each program has been removed before continuing.

**Important:** The order in which you remove the programs is crucial. Some of the entries do not contain any obvious version identification, and you must click the **Change/Remove** button and wait for the Autonomy uninstaller to start in order to identify the version number. This step removes only the added Service Pack and fix pack updates and does not remove the base Content Search Engine software.

8. (Upgrading from version 4.0.1 only) Complete the manual program removal procedure for Content Search Engine 4.0.1 by removing the K2 Dashboard service:
  - a. From a command window, access the following directory: `C:\Program Files\FileNet\ContentEngine\verity\appserver\bin`.
  - b. Enter the following command: `service remove k2`

9. If collections are stored anywhere in the installation path, move the *collections* directory and the *temp* directory to a temporary location outside the installation path.
10. Access the IBM FileNet Content Search Engine installation package.
11. Run the P8CSE-4.5.1.0-WIN.EXE file.
12. Complete the Content Search Engine installation program screens by using the values from your worksheet:
13. Review the following Content Search Engine log files for installation errors. The files are located in the *verity* directory of the installation path:
  - verity\_install\_path*\cse\_install\_log\_4\_5\_1.txt
  - verity\_install\_path*\vconfig.log

It is a best practice to review log files even if the Content Search Engine installation program does not indicate any errors. Some errors noted in the log files are benign. If an error is not benign (that is, you cannot subsequently index or search for documents), refer to the log file for help in determining the cause.
14. Access Windows Services and stop the two running Verity K2 services.
15. Open a command window and change directory to the location of the IBM FileNet Content Search Engine installation package.
16. To restore your configuration from the backup files, run the following commands:
 


```
restore_k2.bat "temporary_location_path" "verity_install_path"
```

where:

  - "temporary\_location-path"* is the temporary path you entered earlier in this procedure when you ran *backup\_k2.bat*.
  - "verity\_install\_path"* is the path to the *verity* directory in the Autonomy K2 installation path.

For example: `restore_k2.bat "C:\temp" "C:\Program Files\IBM\FileNet\ContentEngine\verity"`
17. If you moved collections earlier in this procedure, restore your *collections* directory and *temp* directory to their original locations.
18. For a single-machine configuration, access Windows Services and start the two Autonomy K2 services. For multiserver configurations, do not start the services until all Autonomy K2 servers are upgraded.
19. Access the K2 Dashboard and verify that the services from your previous installation are restored and running.

### 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*.

*Upgrading Content Search Engine silently (Windows):*

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

To upgrade Content Search Engine 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 Search Engine values, filter by **CSE Installer** in the **Installation or Configuration Program** column.

2. Access the Autonomy K2 machine and log on as *k2\_os\_user*.
3. Access Windows Services and stop the two Verity K2 services.
4. Copy the IBM FileNet Content Search Engine installation package to the Autonomy K2 machine.
5. Open a command window and change directory to the location of the IBM FileNet Content Search Engine installation package.
6. Run the following commands:

```
backup_k2.bat "verity_install_path" "temporary_location_path"
```

where:

*"verity\_install\_path"* is the path to the verity directory in the current installation path.

*"temporary\_location\_path"* is the location in which you want to temporarily back up your Autonomy K2 configuration files, outside of the current installation path, and not used by any other application. Files from this backup will be used to restore your existing configuration after you complete the software upgrade.

For example: backup\_k2.bat "C:\Program Files\IBM\FileNet\ContentEngine\verity" "C:\temp"

7. (Upgrading from version 4.0.1 only) Access the Windows control panel and remove, in reverse order of installation, each Autonomy-related entry that is listed in the Add or Remove Programs control panel. Ensure that each program has been removed before continuing.

**Important:** The order in which you remove the programs is crucial. Some of the entries do not contain any obvious version identification, and you must click the **Change/Remove** button and wait for the Autonomy uninstaller to start in order to identify the version number. This step removes only the added Service Pack and fix pack updates and does not remove the base Content Search Engine software.


8. (Upgrading from version 4.0.1 only) Complete the manual program removal procedure for Content Search Engine 4.0.1 by removing the K2 Dashboard service:
  - a. From a command window, access the following directory: C:\Program Files\FileNet\ContentEngine\verity\appserver\bin.
  - b. Enter the following command: `service remove k2`
9. If collections are stored anywhere in the installation path, move the *collections* directory and the *temp* directory to a temporary location outside the installation path.
10. Access the IBM FileNet Content Search Engine installation package.
11. Edit the `CSE_silent_install.txt` file to reflect the appropriate responses for your installation by using the values from your worksheet.
12. Start the Autonomy K2 Master Administration server installer by running the following command:

```
P8CSE-4.5.1.0-WIN.EXE -f CSE_silent_install.txt -i silent
```

**Important:** Ensure that you install to the same path as your previous installation.

13. Review the following Content Search Engine log files for installation errors. The files are located in the `verity` directory of the installation path:  
`verity_install_path\cse_install_log_4_5_1.txt`  
`verity_install_path\vconfig.log`  
 It is a best practice to review log files even if the Content Search Engine installation program does not indicate any errors. Some errors noted in the log files are benign. If an error is not benign (that is, you cannot subsequently index or search for documents), refer to the log file for help in determining the cause.
14. Access Windows Services and stop the two running Verity K2 services.
15. Open a command window and change directory to the location of the IBM FileNet Content Search Engine installation package.
16. To restore your configuration from the backup files, run the following commands:  
`restore_k2.bat "temporary_location_path" "verity_install_path"`  
 where:  
`"temporary_location_path"` is the temporary path you entered earlier in this procedure when you ran `backup_k2.bat`.  
`"verity_install_path"` is the path to the `verity` directory in the Autonomy K2 installation path.  
 For example: `restore_k2.bat "C:\temp" "C:\Program Files\IBM\FileNet\ContentEngine\verity"`
17. If you moved collections earlier in this procedure, restore your *collections* directory and *temp* directory to their original locations.
18. For a single-machine configuration, access Windows Services and start the two Autonomy K2 services. For multiserver configurations, do not start the services until all Autonomy K2 servers are upgraded.
19. Access the K2 Dashboard and verify that the services from your previous installation are restored and running.

#### 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*.

#### Setting the logon user for the K2 Administration Server service (Windows):

To avoid problems when indexing documents using UNC, or viewing UNC-indexed documents, the `k2_os_user` needs to run the K2 Administration Server service.

To set the logon user for the K2 Administration Server service:

1. Open the Windows Services window (for example, on Windows Server 2003, right-click My Computer and choose **Manage** → **Services and Applications** → **Services** select Manage Services and Applications | Services).
2. Select and double-click the Verity K2 6.1 Administration Server service.
3. Click the **Log On** tab, enter the `k2_os_user` user and password under which Autonomy K2 services will run, and click **OK**.

**Important:** Whenever you change the password for the `k2_os_user` account, you must update the password on this tab as well. Otherwise, the K2 Administration Server will not start when you restart the machine. Also,

depending on your domain controller group policy settings, the password for this account may be reset, which will result in logon failures for the K2 Administration Server service when the machine is restarted. To avoid these failures, contact your Windows administrator.

4. Restart the Verity K2 6.1 Administration Server service.

### Updating the style file of user fields:

You must edit the Autonomy K2 style file of user fields to add a data field definition for storing the partitioning value of a document.

To edit the style file:

1. Navigate to the directory in the Content Search Engine software that contains the `style.ufl` file:

#### Windows

```
verity_install_path\data\stylesets\FileNet_FileSystem_PushAPI
```

**UNIX** *verity\_install\_path*/data/stylesets/FileNet\_FileSystem\_PushAPI

2. Open the Autonomy K2 style file of user fields, `style.ufl`, for editing.
3. If it is not already present, add the CEMP definition at the bottom of the file:

```
data-table: fce
{
 fixwidth: cemp_partition_date 4 unsigned-integer
}
```

4. Save your edits and close the file.



---

## Upgrading and configuring Process Engine


Upgrade the Process Engine by performing several pre-upgrade steps, installing the Process Engine software and performing multiple post-upgrade steps.

**Important:** Before you start to upgrade the Process Engine software, ensure that you are at the correct version and fix pack level, as indicated in *Plan and Prepare Your Environment for IBM FileNet P8*.

The pre-upgrade and post-upgrade steps you perform will depend on which version of Process Engine software you are upgrading from.

1. "Completing pre-upgrade Process Engine configuration"  
A number of steps must be completed prior to installing the Process Engine software. The steps vary depending on what release you are upgrading from.
2. "Upgrading Process Engine" on page 400  
Upgrade Process Engine software either interactively or silently.
3. "Upgrading the Content Engine client files on Process Engine servers" on page 416  
Installing or upgrading the Content Engine Client files on all Process Engine enables communication between the Content Engine and the Process Engine. For upgrades from 4.0, you must first remove the Content Engine Client files before upgrading them.
4. "Completing post-upgrade Process Engine configuration" on page 421  
You must perform several procedures to complete the upgrade of all Process Engine data and objects. The steps vary depending on what release you are upgrading from.
5. "Installing Process Engine software updates" on page 437  
After installing Process Engine, software updates such as fix packs or interim fixes might also be required.
6. "Installing the latest Process Engine client files on other IBM FileNet P8 servers (for staged upgrades)" on page 437  
When you upgrade Process Engine server software, you must also upgrade the associated Process Engine Client files installed on other machines running FileNet P8 components, for example, on Content Engine and Application Engine servers.

### Related information

 General requirements for all FileNet P8 Platform systems  
Check to make sure your software is at the correct fix pack level before you upgrade.

---

## Completing pre-upgrade Process Engine configuration

A number of steps must be completed prior to installing the Process Engine software. The steps vary depending on what release you are upgrading from.

"Completing pre-upgrade steps for upgrades from Process Engine Version 3.5" on page 392

Verify that prerequisites have been completed and run a number of pre-upgrade steps before upgrading Process Engine software from Version 3.5.

"Completing pre-upgrade steps for upgrades from Process Engine 4.0 or 4.5" on page 397



Verify that prerequisites have been completed and run a number of pre-upgrade steps before upgrading Process Engine software from Version 4.0 or 4.5.

## Completing pre-upgrade steps for upgrades from Process Engine Version 3.5

Verify that prerequisites have been completed and run a number of pre-upgrade steps before upgrading Process Engine software from Version 3.5.

- Verify that you have a current backup of the Process Engine and Process Engine database.
- Verify that you have run the **vwverify** command on all regions to repair any inconsistencies between database queues and rosters.
- Verify that you have reconciled the Process Engine user security information. This reconciliation and repair of inconsistencies discussed above were a part of the steps described in Preparing Process Engine for upgrade in the Planning guide.
- Determine when to run the upgrade SQL script for Oracle databases. This script must be run by using one of the following methods:
  - Run the script manually before you run the Process Engine installation program.
  - Run the script automatically from the Process Engine installation program, which allows the installation program to prompt for the sys password for Oracle in an xterm window.
  - Run the script automatically from the Process Engine installation program, by running silently using operating system authentication. Use operating system authentication only in a trusted environment or when configured with a local database.
- If you are using a production Process Analyzer, verify that all Process Engine events have been transmitted to Process Analyzer and that the Process Analyzer events have been published. If the events have not been transmitted and published, either before purging from the Process Engine database, or before the Process Engine database upgrade, they will not be available to the Process Analyzer.

**Important:** Do not start the Process Task Manager until specifically told to do so. When you start Task Manager, the database is accessed, which should not be done until the database has been upgraded by using the procedures in “Completing post-upgrade Process Engine configuration” on page 421.

- Purge the event logs and statistic records in the Process Engine database. Clear the event logs and statistics records that are no longer required for Process Engine tracker items or workflow milestones. Clearing these items reduces the amount of time required to upgrade the Process Engine database. If Process Analyzer is installed, complete the steps in Verifying that all Process Engine 3.5 events have been transmitted and Verifying that all Process Analyzer 3.5 events have been published before purging event logs and statistics records.
- 1. “Updating all isolated regions” on page 393  
Update all isolated regions before upgrading the Process Engine software by performing a transfer of the upgrade.cd1 file. This assures that there are no pending transfers.
- 2. “Completing pre-upgrade steps for Process Analyzer installations” on page 393  
For Process Analyzer production installations, perform the following tasks before upgrading Process Engine software from version 3.5 to 4.5.1.

3. "Purging event logs and statistics records" on page 395  
Optionally, purge event log and statistics records before you upgrade to reduce the time necessary for the database upgrade to complete.
4. "Stopping all Process Engine-related services and applications (Windows)" on page 396  
Stop all Process Engine-related services and applications before upgrading from version 3.5.
5. "Stopping all Process Engine-related services and applications (UNIX)" on page 397  
Stop all Process Engine-related services and applications before upgrading from version 3.5.

#### Related tasks

 [Preparing Process Engine for upgrade](#)

For more information about preparing to upgrade, see *Plan and Prepare Your Environment for IBM FileNet P8*.

#### Updating all isolated regions

Update all isolated regions before upgrading the Process Engine software by performing a transfer of the `upgrade.cdl` file. This assures that there are no pending transfers.

1. Restart the Process Engine software by entering the following command:  
`initfnsw -y restart`
2. Save any custom settings for CE\_Operations including the login and password for the adaptor and any user exposed data fields.
3. Change directories to the following location of the `upgrade.cdl` file, depending on your operating system:

Option	Description
Windows	<code>\fnsw_loc\sd</code>
UNIX	<code>/fnsw/local/sd</code>

4. Initiate a transfer on all working isolated regions by entering the following command: `vwtfer -o upgrade.cdl -r XXX`  
where `-r XXX` indicates a region number for a single working region.
5. At the prompt, log on as `pe_service_user`.
6. Repeat for every isolated region.
7. Restore the custom settings for CE\_Operations saved before running the transfer. You will need to restore these custom settings again after completing the steps in "Updating the Process Engine security" on page 427.

#### Completing pre-upgrade steps for Process Analyzer installations

For Process Analyzer production installations, perform the following tasks before upgrading Process Engine software from version 3.5 to 4.5.1.

1. "Verifying that all Process Analyzer 3.5 events have been published"  
Process Analyzer must publish all the events in its VMAEDM database. Verify that all events have been published through the Microsoft Query Analyzer.
2. "Verifying that all Process Engine 3.5 events have been transmitted to Process Analyzer" on page 394  
The steps in this procedure apply only if you are using a production Process Analyzer, they are not necessary for a simulation Process Analyzer.

#### Verifying that all Process Analyzer 3.5 events have been published:

Process Analyzer must publish all the events in its VMAEDM database. Verify that all events have been published through the Microsoft Query Analyzer.

Query for the number of rows in the F\_Events table in the VMAEDM database with PAJobId = 0.

The following is an example of the query on the Process Analyzer database.

Using VMAEDM:

```
Select count(*) from F_Events where PAJobId = 0
```

The above query should return 0. If the query returns anything other than 0, then not all events have been published. In that case, you must leave Process Analyzer running until the query returns 0.

### **Verifying that all Process Engine 3.5 events have been transmitted to Process Analyzer:**

The steps in this procedure apply only if you are using a production Process Analyzer, they are not necessary for a simulation Process Analyzer.

The Process Analyzer gets its data from the Process Engine database. All generated events must be transmitted from Process Engine to Process Analyzer before the upgrade. The following steps must be taken to verify that transmission is complete. Some of these steps must be taken on the Process Engine database, some on the Process Engine server by using the vwtool utility, and some on the Process Analyzer VMAEDM database.

You will query the Process Analyzer VMAEDM database for a date/time value. Date/time values are stored in the Process Engine and Process Analyzer databases in different formats. When a value has been acquired from the Process Analyzer database, you will use vwtool to convert the value to the appropriate format for the Process Engine database. You will then run a query on the Process Engine database by using the converted date/time value as one parameter in the SQL query.

To verify that all Process Engine 3.5 events have been transmitted to Process Analyzer 3.5:

1. Stop Process Engine applications. These applications include any applications that are generating events or running workflows.
2. Keep both Process Engine and Process Analyzer running until all the events from Process Engine are transmitted to Process Analyzer.
3. Complete the following sub-steps to acquire a date/time value from the Process Analyzer database and convert it to an appropriate format for the Process Engine database.
  - a. On the Process Analyzer VMAEDM database, run the following SQL query:

```
select InstallDate from X_SchemaInfo
```

This returns a date and time string, such as 09/11/2006 16:23:59. This string must be converted.
  - b. On the Process Engine server, start the vwtool utility to convert the Process Analyzer data/time string to Process Engine format.
  - c. Enter the following at the **vwtool** prompt:

```
convert
```

Then press *Enter*. The following choice list displays:

- t - Time number to string
  - s - String to time number
  - e - Error tuple to three part
  - p - Three part error to error tuple
  - l - Log event type number to string
  - i - User id to user name
  - n - User name to user id
- d. At the Choice? prompt, enter: s  
and press *Enter*. This converts a string to a time number and returns the following information to indicate what the current date/time mask is, as in:  
Current System Mask: mm/dd.yyy hh:tt:ss  
Time Mask (CR=system mask):
- e. Press *Enter* to accept the default mask.
- f. When prompted to enter the time string (CR="), type the value that was returned from the SQL query ran on Process Analyzer VMAEDM in 3a on page 394. (for example, 09/11/2006 16:23:59). Your input must match the format of the current system mask from 3d above. Then press *Enter* .  
A string value is returned for the date/time entered, which you must make note of for the next set of queries. For example:  
Time...[0x4505F00F].....1158017039 => '09/11/2006 16:23:59'
- g. Get a list of all regions on the disk by typing the following at a **vwtool** prompt:  
regions
- h. When prompted, respond by typing:  
d
- i. For every region, type the following at a **vwtool** prompt:  
reg X  
where X is the region number
- j. Type the following at the **vwtool** prompt:  
config
- k. Locate and make note of the physical table name associated with every event log.
- l. On the Process Engine database, run a SQL query (such as the following example) to verify that no untransmitted events remain in the Process Engine database. You will query for the number of records in every physical table associated with event logs, by using the names you acquired in the previous step. Following is an example of the query syntax:  
Select count(\*) from f\_sw.*physical\_table\_name* where  
F\_AEXmitStat = 1 and F\_TimeStamp > *PAInstallDate*  
where:  
*physical\_table name* is the table name from 3k.  
The *PAInstallDate* is the number returned in 3f.
- Note that the physical table name must be preceeded by f\_sw. in the query.  
The query result must be 0. If the queries do not return 0, not all events have been collected, in which case Process Engine and Process Analyzer must keep running until all the events are transmitted and the queries return 0.

### Purging event logs and statistics records

Optionally, purge event log and statistics records before you upgrade to reduce the time necessary for the database upgrade to complete.

Before you upgrade Process Engine, use the **vwlog** utility to reduce the number of event log and statistics records in the database. This step is optional, but eliminating some of these records can reduce the amount of time necessary for the upgrade to complete. Purging these records can take a significant amount of time, so plan this activity accordingly.

Run the command by logging on with the following service user name:

*pe\_service\_user.*

The following examples show the **vwlog** command syntax. If you use Process Analyzer, do not use the **-P** option when you purge logging records.

*Table 39. vwlog command syntax*

Description	Command
The following command removes the statistics from the specified isolated region.	<code>vwlog -X -r region number</code>
The following command removes all log records from the isolated region. Use this command only if all workflows terminated and you no longer need tracking or milestone information.	<code>vwlog -L -r region number</code>

You can use other parameters for the **vwlog** utility to select log records for deletion that meet specific conditions, such as log records for terminated workflows, for tracker related records, and so on. For more information, see the FileNet P8 help topics under **System Administration** → **Process Engine** → **Administration** → **Administrative tools** → **vwlog**.

## Stopping all Process Engine-related services and applications (Windows)

Stop all Process Engine-related services and applications before upgrading from version 3.5.

1. Log on as fnsw.
2. Set the PPM and any routers to manual startup if they are currently configured to autostart.
3. Stop the following components if they are running:
  - Process Simulator
  - Process Analyzer
  - Custom applications that require a router
  - Component Manager
  - Routers - for Application Engines, Content Engine and custom applications
  - Content Engine
  - Pooled Process Manager (PPM)
  - Process Service
  - Process Task Manager
4. Shut down any active windows displaying Process Engine log files.
5. Enter the following at a command prompt to stop the Process Engine software:

```
initfnsw -y stop
```
6. Enter the following at a command prompt after the FileNet P8 software is shut down.

```
killfnsw -D -y -S
```

7. If the Process Engine server has IBM Tivoli Monitor software running on it, the Process Engine installation program might be unable to overwrite two Process Engine files during an upgrade. Take the following steps to avoid the issue.
  - a. Stop the IBM Tivoli Monitor software.
  - b. Rename the following files:
    - C:\fns\lib\shobj\sysv.dll
    - C:\fns\lib\shobj\fn\_snmpd.dll
  - c. Restart the IBM Tivoli Monitor software.

## Stopping all Process Engine-related services and applications (UNIX)

Stop all Process Engine-related services and applications before upgrading from version 3.5.

1. Log on as root.
2. Set the PPM and any routers to manual startup if they are currently configured to autostart.
3. Stop the following components if they are running:
  - Process Simulator
  - Process Analyzer
  - Custom applications that require a router
  - Component Manager
  - Routers - for Application Engines, Content Engine and custom applications
  - Content Engine
  - Pooled Process Manager (PPM)
  - Process Service
  - Process Task Manager
4. Enter the following at a command prompt after the FileNet P8 software is shut down:
 

```
killfns -DAyS
```

or

```
killfns -D -A -y -S
```
5. (AIX only) Run the following command:
 

```
slibclean
```
6. Run the following command to look for any java processes that are still running:
 

```
ps -ef | grep java | grep VW
```
7. Kill any FileNet P8-related running java processes.

## Completing pre-upgrade steps for upgrades from Process Engine 4.0 or 4.5

Verify that prerequisites have been completed and run a number of pre-upgrade steps before upgrading Process Engine software from Version 4.0 or 4.5.

- Verify that you have a current backup of the Process Engine and Process Engine database.
- Verify that you have run **vwverify** on all regions to repair any inconsistencies between database queues and rosters.
- Determine when to run the upgrade SQL script for Oracle databases. This script must be run in one of the following ways:

- manually, before running the Process Engine installation program.
- automatically, from the Process Engine installation program, allowing the installation program to prompt for the sys password for Oracle in an xterm window.
- automatically, from the Process Engine installation program, running silently by using operating system authentication. Use operating system authentication only in a trusted environment or when configured with a local database.

“Updating all isolated regions”

Update all isolated regions before upgrading the Process Engine software by performing a transfer of the `upgrade.cd1` file. This assures that there are no pending transfers.

“Purging event logs and statistics records” on page 399

Optionally, purge event log and statistics records before you upgrade to reduce the time necessary for the database upgrade to complete.


“Stopping all Process Engine-related services and applications (Windows)” on page 399

Stop all Process Engine-related services and applications before upgrading from version 4.0 or 4.5.

“Stopping all Process Engine-related services and applications (Unix)” on page 400

Stop all Process Engine-related services and applications before upgrading from version 4.0 or 4.5.

**Related tasks**

 **Preparing Process Engine for upgrade**

For more information about preparing to upgrade, see *Plan and Prepare Your Environment for IBM FileNet P8*.

**Updating all isolated regions**

Update all isolated regions before upgrading the Process Engine software by performing a transfer of the `upgrade.cd1` file. This assures that there are no pending transfers.

1. Restart the Process Engine software by entering the following command:  
`initfnsw -y restart`
2. Save any custom settings for CE\_Operations including the login and password for the adaptor and any user exposed data fields.
3. Change directories to the following location of the `upgrade.cd1` file, depending on your operating system:

Option	Description
Windows	<code>\fnsw_loc\sd</code>
UNIX	<code>/fnsw/local/sd</code>

4. Initiate a transfer on all working isolated regions by entering the following command: `vwtfcr -o upgrade.cd1 -r XXX`  
where `-r XXX` indicates a region number for a single working region.
5. At the prompt, log on as `pe_service_user`.
6. Repeat for every isolated region.



- Restore the custom settings for CE\_Operations saved before running the transfer. You will need to restore these custom settings again after completing the steps in “Completing the upgrade from Process Engine 4.0, 4.5.0, or higher” on page 434.

## Purging event logs and statistics records

Optionally, purge event log and statistics records before you upgrade to reduce the time necessary for the database upgrade to complete.

Before you upgrade Process Engine, use the **vwlog** utility to reduce the number of event log and statistics records in the database. This step is optional, but eliminating some of these records can reduce the amount of time necessary for the upgrade to complete. Purging these records can take a significant amount of time, so plan this activity accordingly.

Run the command by logging on with the following service user name:  
*pe\_service\_user*.

The following examples show the **vwlog** command syntax. If you use Process Analyzer, do not use the **-P** option when you purge logging records.

Table 40. vwlog command syntax

Description	Command
The following command removes the statistics from the specified isolated region.	<code>vwlog -X -r region number</code>
The following command removes all log records from the isolated region. Use this command only if all workflows terminated and you no longer need tracking or milestone information.	<code>vwlog -L -r region number</code>

You can use other parameters for the **vwlog** utility to select log records for deletion that meet specific conditions, such as log records for terminated workflows, for tracker related records, and so on. For more information, see the FileNet P8 help topics under **System Administration** → **Process Engine** → **Administration** → **Administrative tools** → **vwlog**.

## Stopping all Process Engine-related services and applications (Windows)

Stop all Process Engine-related services and applications before upgrading from version 4.0 or 4.5.

- Log on as *fns* (or alias).
- Stop the following components if they are running:
  - Process Simulator
  - Process Analyzer
  - Component Manager
  - Content Engine
  - Process Service
  - Process Task Manager
- Shut down any active windows displaying Process Engine log files.
- Enter the following at a command prompt to stop the Process Engine software:  
`initfns -y stop`

5. Enter the following at a command prompt after the Process Engine software is shut down.  

```
killfnsw -D -y -S
```
6. If the Process Engine server has IBM Tivoli Monitor software running on it, the Process Engine installation program might be unable to overwrite two Process Engine files during an upgrade. Take the following steps to avoid the issue.
  - a. Stop the IBM Tivoli Monitor software.
  - b. Rename the following files:  

```
C:\fnsw\lib\shobj\sysv.dll
```

```
C:\fnsw\lib\shobj\fn_snmpd.dll
```
  - c. Restart the IBM Tivoli Monitor software.

### **Stopping all Process Engine-related services and applications (Unix)**

Stop all Process Engine-related services and applications before upgrading from version 4.0 or 4.5.

1. Log on as root.
2. Stop the following components if they are running:
  - Process Simulator
  - Process Analyzer
  - Component Manager
  - Content Engine
  - Process Service
  - Process Task Manager
3. Shut down any active windows displaying Process Engine log files.
4. Enter the following at a command prompt to stop the Process Engine software:  

```
initfnsw -y stop
```
5. Enter the following at a command prompt after the Process Engine software is shut down.  

```
killfnsw -DAYs
```

or

```
killfnsw -D -A -y -S
```
6. (AIX only) Run the following command:  

```
slibclean
```
7. Run the following command to look for any java processes that are still running:  

```
ps -ef | grep java | grep VW
```
8. Kill any FileNet P8-related running java processes.

---

## **Upgrading Process Engine**

Upgrade Process Engine software either interactively or silently.

“Upgrading Process Engine interactively” on page 401

Several Process Engine upgrade screens will display only if the upgrade is from Process Engine version 3.5. Those screens are noted in the Installation and Upgrade Worksheet.

“Upgrading Process Engine silently” on page 408

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

## Upgrading Process Engine interactively

Several Process Engine upgrade screens will display only if the upgrade is from Process Engine version 3.5. Those screens are noted in the Installation and Upgrade Worksheet.

You will find references to logging on as the root and fnsw users within the procedures to upgrade Process Engine software. For all UNIX operating systems, the root user must run in the Bourne or Korn shell and the fnsw user must run in the Korn shell.

**Important:** Before starting the Process Engine installation, verify that you have completed the steps in the To configure your /etc/hosts file section in the *Plan and Prepare Your Environment for IBM FileNet P8*.

To verify the database connection:

1. "Verifying the Process Engine database connection"  
Verify the ability to connect to the Process Engine database. The Process Engine installation program will connect to the database during software installation.
2. "Upgrading Process Engine interactively" on page 404  
You will find references to logging on as the root and fnsw users within the procedures to upgrade Process Engine software. For all UNIX operating systems, the root user must run in the Bourne or Korn shell and the fnsw user must run in the Korn shell.
3. "Setting the f\_maint and f\_sw passwords" on page 406  
Set or reset the passwords for the f\_sw and f\_maint users. This will verify that the encrypted version matches the database or operating system version of the passwords.
4. "Restoring any custom modifications for root and fnsw users (UNIX)" on page 407  
Process Engine installation creates new versions of a number of files. If the previous versions of these files contained any custom settings, edit the new files for the fnsw and root users accordingly.
5. "Editing the /etc/inittab file" on page 407  
By default, the Process Engine software starts automatically when you restart the server and needs its database started beforehand. If the database is not automatically started on server restart, edit the /etc/inittab file on the Process Engine machine to comment out the autostart of Process Engine.

### Verifying the Process Engine database connection

Verify the ability to connect to the Process Engine database. The Process Engine installation program will connect to the database during software installation.

"Verifying the Process Engine database connection (Microsoft SQL Server)" on page 402

Take the following steps to verify that the Microsoft SQL Server database instance used by Process Engine is accessible. Both the Process Engine database and filegroup names are required parameters. Make whatever corrections are necessary before proceeding.

"Verifying the Process Engine database connection (DB2)" on page 402

Verify the connection to the DB2 Process Engine database by executing the following commands to start a command line processor.

"Verifying the Process Engine database connection (Oracle)" on page 403

Verify that the Oracle database instance used by Process Engine is accessible. How you log on to sqlplus will vary, depending upon how you will choose to run the SQL scripts.

### Verifying the Process Engine database connection (Microsoft SQL Server):

Take the following steps to verify that the Microsoft SQL Server database instance used by Process Engine is accessible. Both the Process Engine database and filegroup names are required parameters. Make whatever corrections are necessary before proceeding.

1. Log on to the Process Engine as a member of the local Administrators group or a user with equivalent permissions. The user you log on as must also be a database administrator. If the database is remote, the SQL connection must also be a trusted connection.
2. At a command prompt, enter:  

```
osql -E -D DSN
```

where *DSN* is the ODBC data source name  
This command puts Process Engine into osql interactive mode.
3. At the osql prompt, enter:  

```
1> use VWdb
2> go
```

where *VWdb* is the Process Engine database name  
This command verifies that the Process Engine database has been created. If you get another prompt with no error, you are attached to that database.
4. Verify that the correct Process Engine filegroup was created. At the osql prompt, enter:  

```
1> select substring(groupname,1,20) from sysfilegroups where groupname=
'defined filegroup'
2> go
```

where *defined filegroup* is the default filegroup  
A listing of the Process Engine filegroups will display, for example:  

```

vwdata_fg
```
5. Exit osql by typing **exit**.

### Verifying the Process Engine database connection (DB2):

Verify the connection to the DB2 Process Engine database by executing the following commands to start a command line processor.

1. Log on to the DB2 Control Center tool on the Process Engine, as follows:

#### Windows

At a command prompt, start the DB2 Command Line Processor by typing the following command:

```
db2cmd
```

and, at the subsequently displayed prompt, enter the following command:

```
db2
```

**UNIX** Log on as the client instance owner and run the following at a command prompt:

```
db2
```

2. At the DB2 prompt, enter the following command indicating either the database alias or the instance name:

```
connect to database_alias or instance_name user f_sw using
f_sw password
```

where:

*database\_alias* is the Process Engine DB2 for Linux, UNIX and Windows database alias for remote databases. For local databases, use the database name.

*instance\_name* is the Process Engine DB2 for z/OS database name

*f\_sw* is the Process Engine runtime user, either the default *f\_sw* user or the assigned alias

*f\_sw password* is the runtime user's password.

DB2 will display the database connection information.

The following example shows the database connection command and the information returned:

```
db2 => connect to pedbinst user f_sw using fswpassword
```

```
Database Connection Information
```

```
Database server = DB2/AIX64 9.5.0
```

```
SQL authorization ID = F_SW
```

```
Local database alias = PEDBINST
```

In this example, the database alias is *pedbinst*, the user is *f\_sw*, and the *f\_sw* user password is *fswpassword*.

### Verifying the Process Engine database connection (Oracle):

Verify that the Oracle database instance used by Process Engine is accessible. How you log on to *sqlplus* will vary, depending upon how you will choose to run the SQL scripts.

This procedure will verify that you can connect to the Oracle database in the same way the Process Engine installation program will. Make whatever corrections are necessary before proceeding.

To verify the Process Engine database connection:

1. Run the following at a command prompt on the Process Engine:

```
su - oracle -c "sqlplus"
```

2. Enter one of the following commands at the SQLPlus prompt, as follows:

- If the Process Engine pre-installation SQL scripts will be run from the Process Engine installation program by prompting for the *sys* password, type the following command:

```
sys/password as sysdba
```

- If the SQL scripts will be run from the Process Engine installation program by using operating system authentication, type the following command:

```
/ as sysdba
```

3. At the prompt, enter the following SQL command:

```
SQL> select instance_name, host_name, version
from v$instance;
```

The following represents an example of the information returned:

```
INSTANCE_NAME
```

```

```

```
HOST_NAME
```

```

```

```
VERSION
```

```

```

p8dbshr HQVWBUCS 10.2.0.2.0

where:

- *p8dbshr* is the instance ORACLE\_SID.
- *HQVWBUCS* is the database server name.
- *10.2.0.2.0* is the Oracle server version.

## Upgrading Process Engine interactively

You will find references to logging on as the root and fnsr users within the procedures to upgrade Process Engine software. For all UNIX operating systems, the root user must run in the Bourne or Korn shell and the fnsr user must run in the Korn shell.

Several Process Engine upgrade screens will display only if the upgrade is from Process Engine version 3.5. Those screens are noted in the Installation and Upgrade Worksheet.

“Upgrading the Process Engine software interactively (Windows)”

You can upgrade the Process Engine by using the Process Engine installation wizard.

“Upgrading the Process Engine software interactively (UNIX)” on page 405

You can upgrade the Process Engine by using the Process Engine installation wizard.

### Upgrading the Process Engine software interactively (Windows):

You can upgrade the Process Engine by using the Process Engine installation wizard.

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 Process Engine values, filter by **PE Installer** in the **Installation or Configuration Program** column.

2. Log on as *fnsr*.
3. Navigate to the Process Engine software package, and start the P8PE-4.5.1-WIN.exe installation program. To run the Process Engine installation from disk, you must copy the installation files to a disk volume where 8.3 name generation is enabled, or if 8.3 name generation is disabled, you must copy the installation to a path that uses only short (8.3) names.

When running from disk, either interactively or silently, be aware that the Process Engine installation program has a 64-character path limitation when the path is expressed in 8.3 format. This limitation applies to the IMSInst subdirectory. For example, the original path is:

```
\\server08\Software\InstallationDisks\FileNet\Release P8
4.5.1\ProcessEngine\Windows\IMSInst
```

When expressed in 8.3 format the path might be:

```
\\server08\Software\INSTAL~1\FileNet\RELEAS~1.0\PROCES~1\Windows\IMSInst
```

This compressed path is 73 characters long, exceeding the 64-character limit.


4. Check for any .log files that were generated when the upgrade program ran. The files could be in any of the following locations, depending on whether the upgrade was successful and, if not, where errors occurred. Correct any errors or failures indicated before proceeding to the next step.
  - C:\Program Files\IBM\FileNet\PE\PE451\_setup.log
  - C:\Program Files\IBM\FileNet\PE

- C:\FNSW\tmp\_installer
  - C:\Program Files\IBM\FileNet\IS\mini\_installer.log, Windows Event logs, and log files under \FNSW\_LOC\logs
  - For 64-bit Windows, these paths will be C:\Program Files(x86)\..
5. Start the following services:
- IMS ControlService
  - Process Engine Services Manager

### 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*.

### Upgrading the Process Engine software interactively (UNIX):

You can upgrade the Process Engine by using the Process Engine installation wizard.

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 Process Engine values, filter by **PE Installer** in the **Installation or Configuration Program** column.


2. Log on to the Process Engine server as the root user. If you plan to run the SQL scripts from the Process Engine installation program, you must log on as a database administrator.
3. Navigate to the Process Engine software package.
4. From the console, launch the appropriate P8PE-4.5.1-*platform*.bin installation program and wait for the files to finish unpacking.

Platform	Command
AIX	P8PE-4.5.1-AIX.BIN
HPUX	P8PE-4.5.1-HPUX.BIN
HPUXi	P8PE-4.5.1-HPUXI.BIN
Solaris	P8PE-4.5.1-SOL.BIN

5. Monitor /fnsw/local/logs/wizard to check the progress of the upgrade since the installation program will run for several minutes and its progress, though displayed, might not visibly advance for an extended period of time. Reboot when prompted.
6. Check for any .log files that were generated when the upgrade program ran. The files could be in any of the following locations, depending on whether the upgrade was successful and, if not, where errors occurred. Correct any errors or failures indicated before proceeding to the next step.
  - /fnsw/local/logs/PE (if the install completes successfully)
  - /fnsw/tmp\_installer/PE451\_setup.log (if the install has errors)
  - /fnsw/local/logs/wizard/*date\_time.log* and other subdirectories under /fnsw/local/logs
7. Log off as the root user and log on as *fnsww*.



## 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*.

## Setting the f\_maint and f\_sw passwords

Set or reset the passwords for the f\_sw and f\_maint users. This will verify that the encrypted version matches the database or operating system version of the passwords.

“Setting the f\_maint and f\_sw passwords (DB2)”

For added security, Process Engine stores an encrypted version of the passwords for the f\_sw and f\_maint users, or their aliases, in a file called rdbup.bin.

“Setting the f\_maint and f\_sw passwords (Oracle and Microsoft SQL Server)”

For added security, Process Engine stores an encrypted version of the passwords for the f\_sw and f\_maint users, or their aliases, in a file called rdbup.bin. This is in addition to passwords for these users in the Oracle or Microsoft SQL Server database. The encrypted password and the database user's passwords must match.

### Setting the f\_maint and f\_sw passwords (DB2):

For added security, Process Engine stores an encrypted version of the passwords for the f\_sw and f\_maint users, or their aliases, in a file called rdbup.bin.

To verify that the passwords match between the encrypted file and the operating system, you can use the Xdbconnect utility. Xdbconnect works only if the passwords in the encrypted file and the database match.

You must change the passwords for the f\_maint and f\_sw users. For DB2, the encrypted file will be updated.

On UNIX, several Process Engine utilities are setuid fns (or its alias), and will therefore run with that user's X Window settings regardless of which user is currently logged on.

1. Log on as the fns user.
2. Start the Database Server Connect application by executing the following:  
`Xdbconnect -r`
3. Change the primary password for the users f\_sw and f\_maint to match the operating system user password.
4. Exit the application.

### Setting the f\_maint and f\_sw passwords (Oracle and Microsoft SQL Server):

For added security, Process Engine stores an encrypted version of the passwords for the f\_sw and f\_maint users, or their aliases, in a file called rdbup.bin. This is in addition to passwords for these users in the Oracle or Microsoft SQL Server database. The encrypted password and the database user's passwords must match.

To verify that the passwords match between the encrypted file and the Oracle or SQL Server database, use the following procedure to start the Xdbconnect utility. Xdbconnect works only if the passwords in the encrypted file and the database match.

You must change the passwords for the `f_maint` and `f_sw` users. For Oracle and Microsoft SQL Server databases, both the encrypted file and the database passwords are updated.

On UNIX, several Process Engine utilities are configured with `setuid fnsfw`. (or its alias), and will therefore run with that user's X Window settings, regardless of which user is currently logged on.

1. Log on as the `fnsfw` user.
2. Start the Database Server Connect application by running the following command: `Xdbconnect -r`
3. Change the primary password for the users `f_sw` and `f_maint` to match the database password.
4. Exit the application.

### Restoring any custom modifications for root and fnsfw users (UNIX)

Process Engine installation creates new versions of a number of files. If the previous versions of these files contained any custom settings, edit the new files for the `fnsfw` and `root` users accordingly.

Saved files are in `.filename.old.nn`, where `nn` is a sequential number. The latest saved version will be in the highest numbered file. The following files are modified by the Process Engine installation program:

- `.Xdefaults`
- `.Xresources`
- `.dbxinit`
- `.dtprofile`
- `.env`
- `.login`
- `.mwmrc`
- `.xinitrc`
- `.profile`
- `.cshrc`

### Editing the `/etc/inittab` file

By default, the Process Engine software starts automatically when you restart the server and needs its database started beforehand. If the database is not automatically started on server restart, edit the `/etc/inittab` file on the Process Engine machine to comment out the autostart of Process Engine.

The following are examples of changes to make.

*Table 41. Changes to make to the `/etc/inittab` file*

Operating system:	Changes to make:
AIX	Change: <pre>rcfnsfw:2:once:/etc/rc.initfnsfw 2&gt;&amp;1   alog -tboot &gt; /dev/console 2&gt;&amp;1</pre> to read: <pre>:rcfnsfw:2:once:/etc/rc.initfnsfw 2&gt;&amp;1   alog -tboot &gt; /dev/console 2&gt;&amp;1</pre>

Table 41. Changes to make to the /etc/inittab file (continued)

Operating system:	Changes to make:
HPUX	Change: <pre>rcfn:2:once:/etc/rc.initfnsw 2&gt;&amp;1   alog -tboot &gt; /dev/console 2&gt;&amp;1</pre> to read: <pre>#rcfn:2:once:/etc/rc.initfnsw 2&gt;&amp;1   alog -tboot &gt; /dev/console 2&gt;&amp;1</pre>
Solaris	Change: <pre>fn:3:wait:/bin/sh /etc/rc.initfnsw &lt;/dev/console &gt;/dev/console 2&gt;&amp;1</pre> to read: <pre>#fn:3:wait:/bin/sh /etc/rc.initfnsw &lt;/dev/console &gt;/dev/console 2&gt;&amp;1</pre>

## Upgrading Process Engine silently

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

**Important:** Before starting the Process Engine installation, verify that you have completed the steps in the To configure your /etc/hosts file section in the *Plan and Prepare Your Environment for IBM FileNet P8*.

1. "Verifying the Process Engine database connection"  
Verify the ability to connect to the Process Engine database. The Process Engine installation program will connect to the database during software installation.
2. "Upgrading Process Engine silently" on page 411  
You will find references to logging on as the root and fnsw users within the procedures to upgrade Process Engine software. For all UNIX operating systems, the root user must run in the Bourne or Korn shell and the fnsw user must run in the Korn shell.
3. "Setting the f\_maint and f\_sw passwords" on page 414  
Set or reset the passwords for the f\_sw and f\_maint users. This will verify that the encrypted version matches the database or operating system version of the passwords.
4. "Restoring any custom modifications for root and fnsw users (UNIX)" on page 415  
Process Engine installation creates a new versions of a number of files. If the previous versions of these files contained any custom settings, edit the new files for the fnsw and root users accordingly.
5. "Editing the /etc/inittab file" on page 415  
By default, the Process Engine software starts automatically when you restart the server and needs its database started beforehand. If the database is not automatically started on server restart, edit the /etc/inittab file on the Process Engine machine to comment out the autostart of Process Engine.

### Verifying the Process Engine database connection

Verify the ability to connect to the Process Engine database. The Process Engine installation program will connect to the database during software installation.

"Verifying the Process Engine database connection (Microsoft SQL Server)" on page 409

Take the following steps to verify that the Microsoft SQL Server database instance used by Process Engine is accessible. Both the Process Engine database and filegroup names are required parameters. Make whatever corrections are necessary before proceeding.

“Verifying the Process Engine database connection (DB2)”

Verify the connection to the DB2 Process Engine database by using the DB2 Control Center tool, or by running the following commands.

“Verifying the Process Engine database connection (Oracle)” on page 410

verify that the Oracle database instance used by Process Engine is accessible.

How you log on to sqlplus will vary, depending upon how you will choose to run the SQL scripts.

### Verifying the Process Engine database connection (Microsoft SQL Server):

Take the following steps to verify that the Microsoft SQL Server database instance used by Process Engine is accessible. Both the Process Engine database and filegroup names are required parameters. Make whatever corrections are necessary before proceeding.

1. Log on to the Process Engine as a member of the local Administrators group or a user with equivalent permissions. The user you log on as must also be a database administrator. If the database is remote, the SQL connection must also be a trusted connection.

2. At a command prompt, enter:

```
osql -E -D DSN
```

where *DSN* is the ODBC data source name

This command puts Process Engine into osql interactive mode.

3. At the osql prompt, enter:

```
1> use VWdb
```

```
2> go
```

where *VWdb* is the Process Engine database name

This command verifies that the Process Engine database has been created. If you get another prompt with no error, you are attached to that database.

4. Verify that the correct Process Engine filegroup was created. At the osql prompt, enter:

```
1> select substring(groupname,1,20) from sysfilegroups where groupname=
'defined filegroup'
```

```
2> go
```

where *defined filegroup* is the default filegroup

A listing of the Process Engine filegroups will display, for example:

```
vwdata_fg
```

5. Exit osql by typing **exit**.

### Verifying the Process Engine database connection (DB2):

Verify the connection to the DB2 Process Engine database by using the DB2 Control Center tool, or by running the following commands.

1. Log on to the DB2 Control Center tool on the Process Engine, as follows:

#### Windows

At a command prompt, start the DB2 Command Line Processor by typing the following command:

```
db2cmd
```

and, at the subsequently displayed prompt, enter the following command:

```
db2
```

**UNIX** Log on as the client instance owner and run the following at a command prompt:

```
db2
```

2. At the DB2 prompt, enter the following command indicating either the database alias or the instance name:

```
connect to database_alias or instance_name user f_sw using
f_sw password
```

where:

*database\_alias* is the Process Engine DB2 for Linux, UNIX and Windows database alias for remote databases. For local databases, use the database name.

*instance\_name* is the Process Engine DB2 for z/OS database name

*f\_sw* is the Process Engine runtime user, either the default *f\_sw* user or the assigned alias

*f\_sw password* is the runtime user's password.

DB2 will display the database connection information.

The following example shows the database connection command and the information returned:

```
db2 => connect to pedbinst user f_sw using fswpassword
```

```
Database Connection Information
```

```
Database server = DB2/AIX64 9.5.0
```

```
SQL authorization ID = F_SW
```

```
Local database alias = PEDBINST
```

In this example, the database alias is pedbinst, the user is *f\_sw*, and the *f\_sw* user password is fswpassword.

### Verifying the Process Engine database connection (Oracle):

verify that the Oracle database instance used by Process Engine is accessible. How you log on to sqlplus will vary, depending upon how you will choose to run the SQL scripts.

This procedure will verify that you can connect to the Oracle database in the same way the Process Engine installation program will. Make whatever corrections are necessary before proceeding.

To verify the Process Engine database connection:

1. Run the following at a command prompt on the Process Engine:

```
su - oracle -c "sqlplus"
```

2. Enter one of the following commands at the SQLPlus prompt, as follows:

- If the Process Engine pre-installation SQL scripts will be run from the Process Engine installation program by prompting for the sys password, type the following command:

```
sys/password as sysdba
```

- If the SQL scripts will be run from the Process Engine installation program by using operating system authentication, type the following command:

```
/ as sysdba
```

3. At the prompt, enter the following SQL command:

```
SQL> select instance_name, host_name, version
from v$instance;
```

The following represents an example of the information returned:

```
INSTANCE_NAME

HOST_NAME

VERSION

p8dbshr HQVWBUCS 10.2.0.2.0
```

where:

- *p8dbshr* is the instance ORACLE\_SID.
- *HQVWBUCS* is the database server name.
- *10.2.0.2.0* is the Oracle server version.

## Upgrading Process Engine silently

You will find references to logging on as the root and fnsr users within the procedures to upgrade Process Engine software. For all UNIX operating systems, the root user must run in the Bourne or Korn shell and the fnsr user must run in the Korn shell.

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

“Upgrading the Process Engine software silently (Windows)”

Take the following steps to silently upgrade Process Engine.

“Upgrading the Process Engine software silently (UNIX)” on page 412

Take the following steps to silently upgrade Process Engine.

“Encrypting passwords for Process Engine” on page 413

Several passwords are required to configure Process Engine components. To accommodate your security requirements, you can encrypt these passwords before you enter them into the configuration files.

## Upgrading the Process Engine software silently (Windows):

Take the following steps to silently upgrade Process 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 Process Engine values, filter by **PE Installer** in the **Installation or Configuration Program** column.

2. Log on as *fnsr*.
3. Navigate to the Process Engine software package.
4. Edit the `PE_silent_install.txt` file to reflect the appropriate responses for your installation. All passwords in the response file must be encrypted.
5. Save the edited response file to your temporary directory.
6. Navigate to the temporary directory on the local disk.
7. Open a command prompt and start the installation program:  
`P8PE-4.5.1-WIN.exe -silent -options PE_silent_install.txt`
8. Check for any `.log` files that were generated when the upgrade program ran. The files could be in any of the following locations, depending on whether the


upgrade was successful and, if not, where errors occurred. Correct any errors or failures indicated before proceeding to the next step.

- C:\Program Files\IBM\FileNet\PE\PE451\_setup.log
- C:\Program Files\IBM\FileNet\PE
- C:\FNSW\tmp\_installer
- C:\Program Files\IBM\FileNet\IS\mini\_installer.log, Windows Event logs, and log files under \FNSW\_LOC\logs
- For 64-bit Windows, these paths will be C:\Program Files(x86)\..

9. Start the following services:

- IMS ControlService
- Process Engine Services Manager

### 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

“Encrypting passwords for Process Engine” on page 413

Several passwords are required to configure Process Engine components. To accommodate your security requirements, you can encrypt these passwords before you enter them into the configuration files.

### Upgrading the Process Engine software silently (UNIX):

Take the following steps to silently upgrade Process 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 Process Engine values, filter by **PE Installer** in the **Installation or Configuration Program** column.

2. Log on to the Process Engine server as the root user. If you plan to run the SQL scripts from the Process Engine installation program, you must log on as a database administrator.
3. Edit the PE\_silent\_install.txt file to reflect the appropriate responses for your installation. All passwords in the response file must be encrypted.
4. Save the edited response file to your temporary directory.
5. Navigate to the temporary directory on the local disk.
6. From the console, launch the appropriate P8PE-4.5.1-*platform*.bin installation program.

Platform	Command
AIX	P8PE-4.5.1-AIX.BIN -silent -options PE_silent_install.txt
HPUX	P8PE-4.5.1-HPUX.BIN -silent -options PE_silent_install.txt
HPUXi	P8PE-4.5.1-HPUXI.BIN -silent -options PE_silent_install.txt
Solaris	P8PE-4.5.1-SOL.BIN -silent -options PE_silent_install.txt



7. Monitor `/fnsw/local/logs/wizard` to check the progress of the upgrade since installation will run for several minutes, and its progress, though displayed, might not visibly advance for an extended period of time.
8. Check for any `.log` files that were generated when the upgrade program ran. The files could be in any of the following locations, depending on whether the upgrade was successful and, if not, where errors occurred. Correct any errors or failures indicated before proceeding to the next step.
  - `/fnsw/local/logs/PE` (if the install completes successfully)
  - `/fnsw/tmp_installer/PE451_setup.log` (if the install has errors)
  - `/fnsw/local/logs/wizard/date_time.log` and other subdirectories under `/fnsw/local/logs`
9. Log off as the root user and log on as `fnsw` (or the alias).

### Related concepts

 [Encrypting passwords for Process Engine](#)

For more information about encrypting passwords for Process Engine, see the *Plan and Prepare Your Environment for IBM FileNet P8*.

### Related tasks

“Encrypting passwords for Process Engine”

Several passwords are required to configure Process Engine components. To accommodate your security requirements, you can encrypt these passwords before you enter them into the configuration files.

### Encrypting passwords for Process Engine:

Several passwords are required to configure Process Engine components. To accommodate your security requirements, you can encrypt these passwords before you enter them into the configuration files.

Ensure that Java is installed and that the location to your Java runtime environment (JRE) is in your `PATH` environment variable.

1. Copy the following files from the `\Tools` directory on the installation media for Process Engine software to a local drive:
  - `fnencryptutils` - an executable `.jar` file
  - `RunEncryptApp` - a batch file
2. Run one of the following executable files to start the password application:

Option	Description
Windows	<code>RunEncryptApp.bat</code>
UNIX	<code>RunEncryptApp.sh</code>

3. Enter the appropriate values for the user name and password.
4. Reenter the password to confirm it.
5. Click **Generate**.
6. An encrypted password will be generated and displayed in the encrypted password field.
7. Copy and paste this password into the appropriate configuration file.

## Related tasks

“Upgrading the Process Engine software silently (UNIX)” on page 412  
Take the following steps to silently upgrade Process Engine.

“Upgrading the Process Engine software silently (Windows)” on page 411  
Take the following steps to silently upgrade Process Engine.

## Setting the f\_maint and f\_sw passwords

Set or reset the passwords for the f\_sw and f\_maint users,. This will verify that the encrypted version matches the database or operating system version of the passwords.

### “Setting the f\_maint and f\_sw passwords (DB2)”

For added security, Process Engine stores an encrypted version of the passwords for the f\_sw and f\_maint users, or their aliases, in a file called rdbup.bin.

### “Setting the f\_maint and f\_sw passwords (Oracle and Microsoft SQL Server)”

For added security, Process Engine stores an encrypted version of the passwords for the f\_sw and f\_maint users, or their aliases, in a file called rdbup.bin. This is in addition to passwords for these users in the Oracle or Microsoft SQL Server database. The encrypted password and the database user's passwords must match.

### Setting the f\_maint and f\_sw passwords (DB2):

For added security, Process Engine stores an encrypted version of the passwords for the f\_sw and f\_maint users, or their aliases, in a file called rdbup.bin.

To verify that the passwords match between the encrypted file and the operating system, you can use the Xdbconnect utility. Xdbconnect works only if the passwords in the encrypted file and the database match.

You must change the passwords for the f\_maint and f\_sw users. For DB2, the encrypted file will be updated.

On UNIX, several Process Engine utilities are setuid fns (or its alias), and will therefore run with that user's X Window settings regardless of which user is currently logged on.

1. Log on as the fns user.
2. Start the Database Server Connect application by executing the following:  
`Xdbconnect -r`
3. Change the primary password for the users f\_sw and f\_maint to match the operating system user password.
4. Exit the application.

### Setting the f\_maint and f\_sw passwords (Oracle and Microsoft SQL Server):

For added security, Process Engine stores an encrypted version of the passwords for the f\_sw and f\_maint users, or their aliases, in a file called rdbup.bin. This is in addition to passwords for these users in the Oracle or Microsoft SQL Server database. The encrypted password and the database user's passwords must match.

To verify that the passwords match between the encrypted file and the Oracle or SQL Server database, use the following procedure to start the Xdbconnect utility. Xdbconnect works only if the passwords in the encrypted file and the database match.

You must change the passwords for the `f_maint` and `f_sw` users. For Oracle and Microsoft SQL Server databases, both the encrypted file and the database passwords are updated.

On UNIX, several Process Engine utilities are configured with `setuid fnsw`. (or its alias), and will therefore run with that user's X Window settings, regardless of which user is currently logged on.

1. Log on as the `fnsw` user.
2. Start the Database Server Connect application by running the following command: `Xdbconnect -r`
3. Change the primary password for the users `f_sw` and `f_maint` to match the database password.
4. Exit the application.

### Restoring any custom modifications for root and fnsw users (UNIX)

Process Engine installation creates a new versions of a number of files. If the previous versions of these files contained any custom settings, edit the new files for the `fnsw` and `root` users accordingly.

Saved files are in `.filename.old.nn`, where `nn` is a sequential number. The latest saved version will be in the highest numbered file. The following files are modified by the Process Engine installation program:

- `.Xdefaults`
- `.Xresources`
- `.dbxinit`
- `.dtprofile`
- `.env`
- `.login`
- `.mwmrc`
- `.xinitrc`
- `.profile`
- `.cshrc`

### Editing the `/etc/inittab` file

By default, the Process Engine software starts automatically when you restart the server and needs its database started beforehand. If the database is not automatically started on server restart, edit the `/etc/inittab` file on the Process Engine machine to comment out the autostart of Process Engine.

The following are examples of changes to make.

*Table 42. Changes to make to the `/etc/inittab` file*

Operating system:	Changes to make:
AIX	Change: <pre>rcfnsw:2:once:/etc/rc.initfnsw 2&gt;&amp;1   alog -tboot &gt; /dev/console 2&gt;&amp;1</pre> to read: <pre>:rcfnsw:2:once:/etc/rc.initfnsw 2&gt;&amp;1   alog -tboot &gt; /dev/console 2&gt;&amp;1</pre>

Table 42. Changes to make to the /etc/inittab file (continued)

Operating system:	Changes to make:
HPUX	Change: rcfn:2:once:/etc/rc.initfnsw 2>&1   alog -tboot > /dev/console 2>&1  to read: #rcfn:2:once:/etc/rc.initfnsw 2>&1   alog -tboot > /dev/console 2>&1
Solaris	Change: fn:3:wait:/bin/sh /etc/rc.initfnsw </dev/console >/dev/console 2>&1  to read: #fn:3:wait:/bin/sh /etc/rc.initfnsw </dev/console >/dev/console 2>&1

## Upgrading the Content Engine client files on Process Engine servers

Installing or upgrading the Content Engine Client files on all Process Engine enables communication between the Content Engine and the Process Engine. For upgrades from 4.0, you must first remove the Content Engine Client files before upgrading them.

1. “Uninstalling Content Engine client 4.0.x instances”  
If you have the 4.0 version of the Content Engine client files installed, you must remove them before you run the upgrade installation to version 4.5.1. You must remove the 4.0 Content Engine client file for all Process Engine server machines.
2. “Upgrading the Content Engine client files” on page 417  
Installing or upgrading the Content Engine client files on all Process Engine enables communication between the Content Engine and the Process Engine. You can install these files interactively by using the installation wizard, or silently by using the command line and a silent input file.

### Uninstalling Content Engine client 4.0.x instances

If you have the 4.0 version of the Content Engine client files installed, you must remove them before you run the upgrade installation to version 4.5.1. You must remove the 4.0 Content Engine client file for all Process Engine server machines.

“Uninstalling Content Engine Client 4.0.x instances on Windows”

You can use the Microsoft Windows Control Panel to remove the 4.0 version of the Content Engine Client files from your Windows Process Engine Server machines.

“Uninstalling Content Engine Client 4.0 instances on UNIX” on page 417

You must use the uninstaller tools to remove the 4.0 version of the Content Engine client files from your UNIX Process Engine server machines.

### Uninstalling Content Engine Client 4.0.x instances on Windows

You can use the Microsoft Windows Control Panel to remove the 4.0 version of the Content Engine Client files from your Windows Process Engine Server machines.

Depending on the Content Engine client fix pack versions that you have installed, you might have more than one instance of the Content Engine client 4.0 installed. Additionally, the version 4.0 Content Engine client installer supported installing

multiple instance of the Content Engine client on the same server. You must uninstall all instances before upgrading to the 4.5.1 version of Content Engine client.

1. Locate and uninstall all instances of the Content Engine client on the Process Engine server.
2. On the Process Engine, select **Start** → **Settings** → **Control Panel** → **Add/Remove Programs** .
3. Select *Content Engine Client Updater* or *IBM FileNet Content Engine Client Installer* , depending on the fix pack version of Content Engine client that is installed.  
Prior to fix pack P8CE-4.0.1-006: *The Content Engine Client is named* Content Engine Client Updater.  
As of fix pack P8CE-4.0.1-006: *The Content Engine Client is named* IBM FileNet Content Engine Client Installer.
4. Click **Change/Remove** to start the uninstaller.
5. In the Uninstall IBM FileNet Client Installer screen, click **Next**.
6. In the Select Components screen, select **Complete Uninstall**. Click **Next**.
7. In the Uninstall Complete screen, click **Done**.
8. Repeat the steps for each additional instance of *Content Engine Client Updater* or *IBM FileNet Content Engine Client Installer* listed in Add/Remove Programs list.

### Uninstalling Content Engine Client 4.0 instances on UNIX

You must use the uninstaller tools to remove the 4.0 version of the Content Engine client files from your UNIX Process Engine server machines.

Depending on the Content Engine client fix pack versions that you have installed, you might have more than one instance of the Content Engine client 4.0 installed. Additionally, the version 4.0 Content Engine client installer supported installing multiple instance of the Content Engine client on the same server. You must uninstall all instances before upgrading to the 4.5.1 version of Content Engine client.

1. Locate and uninstall all instances of the Content Engine client on the Process Engine server.
2. Run one of the following commands, depending on the fix pack version of Content Engine client that is installed.

Option	Description
Prior to fix pack P8CE-4.0.1-006	<code>/ce_client_install_path/ClientUpdater/_uninst/uninstaller.bin</code>
As of fix pack P8CE-4.0.1-006	<code>/ce_client_install_path/CEClient/_CEClientuninst/uninstaller</code>

3. In the Uninstall IBM FileNet Client Installer screen, click **Next** .
4. In the Select Components screen, select **Complete Uninstall**. Click **Next**.
5. In the Uninstall Complete screen, click **Done**.
6. Repeat the uninstallation steps for each installed instance of Content Engine client on this server.
- 7.

### Upgrading the Content Engine client files

Installing or upgrading the Content Engine client files on all Process Engine enables communication between the Content Engine and the Process Engine. You

can install these files interactively by using the installation wizard, or silently by using the command line and a silent input file.

“Upgrading the latest Content Engine client files on Process Engine servers interactively”

The installation wizard provides an interactive way to install the Content Engine client files. You can use the values you collected on your worksheet to fill in the required value for each field on the wizard screens.

“Upgrading the latest Content Engine client files on Process Engine servers silently” on page 419

The command line method provides a way to silently install the Content 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 Content Engine parameter values, see *Plan and Prepare Your Environment for IBM FileNet P8*.

## Upgrading the latest Content Engine client files on Process Engine servers interactively

The installation wizard provides an interactive way to install the Content Engine client files. You can use the values you collected on your worksheet to fill in the required value for each field on the wizard screens.

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

To install the Content Engine client 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 Content Engine values, filter by **CE Client Installer** in the **Installation or Configuration Program** column.

2. To download the latest software updates, and to determine which of these updates might be required for use with other components and expansion products, contact your service representative.
3. On the machine where Process Engine is installed, log on as fnsw, with these permissions:
  - Read and write permission to a temporary directory, such as *temp* (Windows) or *tmp* (UNIX), on the machine where Process Engine is installed
  - Execute permission on the Content Engine Client install software

The default password for fnsw was BPMtemp1pzwd.

4. Verify that there is a current backup of Process Engine.
5. Copy the Content Engine Client install software from the Content Engine installation software to the temporary directory, and unzip the software package. The version of the installation software must match the version of Content Engine.
6. Access the IBM FileNet P8 Content Engine Client update software.
7. Run one of the commands in the table below, *CE\_version* is the version of Content Engine you intend to run, for example, 4.5.1.


Operating System	Install Program
AIX	P8CE-CLIENT- <i>CE_version</i> -AIX.BIN

Operating System	Install Program
HPUX	P8CE-CLIENT-CE_version -HPUX.BIN
HPUXi	P8CE-CLIENT-CE_version -HPUXI.BIN
Solaris	P8CE-CLIENT-CE_version -SOL.BIN
Windows	P8CE-CLIENT-CE_version -WIN.EXE

- Complete the installation program wizard by using the values from your worksheet.
- When the installation completes, check the Content 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 Engine Client files:

Operating System	Path to Log File
UNIX	/opt/IBM/FileNet/CEClient/ ceclient_install_log_4_5_1.txt
Windows	C:\Program Files\IBM\FileNet\CEClient\ ceclient_install_log_4_5_1.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*.

### Upgrading the latest Content Engine client files on Process Engine servers silently

The command line method provides a way to silently install the Content 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.

To install the Content Engine client files:

- 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 **CE Client Installer** in the **Installation or Configuration Program** column.

- To download the latest software updates, and to determine which of these updates might be required for use with other components and expansion products, contact your service representative.
- On the machine where Process Engine is installed, log on as fnsfw, with these permissions:
  - Read and write permission to a temporary directory, such as *temp* (Windows) or *tmp* (UNIX), on the machine where Process Engine is installed
  - Execute permission on the Content Engine Client install software

The default password for fnsfw was BPMtemp1pzwtd.
- Verify that there is a current backup of Process Engine.



5. Copy the Content Engine Client install software from the Content Engine installation software to the temporary directory, and unzip the software package. The version of the installation software must match the version of Content Engine.
6. Make a back up copy of the CEClient\_silent\_install.txt input file.
7. 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.
8. Navigate to the path containing the Content Engine Client installation program, and run one of the commands in the following table to perform the silent install, where:
9. Copy the Content Engine Client install software from the Content Engine installation software to the temporary directory, and unzip the software package. The version of the installation software must match the version of Content Engine.

*CE\_version* is the version of Content Engine you intend to run, for example, 4.5.1.

*path* is the path that contains the installation program.

Operating System	Install Program
AIX	P8CE-CLIENT- <i>CE_version</i> -AIX.BIN -f <i>path</i> /CECLIENT.AIX/ CEClient_silent_install.txt -i silent
HPUX	P8CE-CLIENT- <i>CE_version</i> -HPUX.BIN -f <i>path</i> /CEClient.HPUX/ CEClient_silent_install.txt -i silent
HPUXi	P8CE-CLIENT- <i>CE_version</i> -HPUXI.BIN -f <i>path</i> /CEClient.HPUXI/ CEClient_silent_install.txt -i silent
Solaris	P8CE-CLIENT- <i>CE_version</i> -SOL.BIN -f <i>path</i> /CEClient.Solaris/ CEClient_silent_install.txt -i silent
Windows	P8CE-CLIENT- <i>CE_version</i> -WIN.EXE -f <i>path</i> \CEClient.Windows\ CEClient_silent_install.txt -i silent

10. When the installation completes, check the Content 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 Engine Client files:


Operating System	Path to Log File
UNIX	/opt/IBM/FileNet/CEClient/ ceclient_install_log_4_5_1.txt
Windows	C:\Program Files\IBM\FileNet\CEClient\ ceclient_install_log_4_5_1.txt

11. When the installation completes, check the Content 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 Engine Client files:

Operating System	Path to Log File
UNIX	/opt/IBM/FileNet/CEClient/ ceclient_install_log_4_5_1.txt

Operating System	Path to Log File
Windows	C:\Program Files\IBM\FileNet\CEClient\ceclient_install_log_4_5_1.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*.

---

## Completing post-upgrade Process Engine configuration

You must perform several procedures to complete the upgrade of all Process Engine data and objects. The steps vary depending on what release you are upgrading from.

“Completing the upgrade from Process Engine 3.5”

Complete the following tasks when upgrading Process Engine from Version 3.5.

“Completing the upgrade from Process Engine 4.0, 4.5.0, or higher” on page 434

Perform the following steps to update a Process Engine database to version 4.5.1. A database update will take place automatically by restarting the software.

### Completing the upgrade from Process Engine 3.5

Complete the following tasks when upgrading Process Engine from Version 3.5.

1. “Completing the upgrade from Process Engine 3.5 by database type” on page 422  
Complete the following tasks when upgrading Process Engine from Version 3.5.
2. “Removing existing routers in Process Task Manager” on page 427  
The Process Routers displayed in Process Task Manager are not used and have no effect on the system other than to cause a warning message on Process Task Manager startup.
3. “Updating the Process Engine security” on page 427  
Update the Process Engine security by using the **vwtaskman** tool.
4. “Running post-upgrade scripts Microsoft SQL Server and DB2” on page 429  
Run two post-upgrade scripts. For each database type, the first script copies records from archived event-log tables to the new 4.5 version of the tables, and the second script deletes the archived log tables, thereby saving database space.
5. “Configuring contiguous free memory for Process Engine (Windows)” on page 431  
Use the procedure in this task to enable Process Engine to use the largest available contiguous free memory area for shared memory allocations. Unless you perform this procedure, at some point during normal execution the system will not allocate shared memory and will cease to function correctly.
6. “Migrating routers and updating isolated regions” on page 432  
Convert all routers to connection points and assign passwords to any existing isolated regions.
7. “Updating email notification” on page 433  
Enable email notification in order to use it. Process Engine also supports localized email notification.
8. “Backing up the database and restarting software” on page 434  
Back up and restart the database software after upgrading.

## Completing the upgrade from Process Engine 3.5 by database type

Complete the following tasks when upgrading Process Engine from Version 3.5.

“Completing the upgrade from Process Engine 3.5 (Oracle)”

Complete the upgrade by initiating an automatic schema change in the database.

“Completing the upgrade from Process Engine 3.5 (DB2)” on page 423

The format of the event log files changed. As a part of this upgrade, several SQL scripts must be executed for DB2 databases.

“Completing the upgrade from Process Engine 3.5 (SQL Server)” on page 425

The format of the event log files have changed. As a part of this upgrade, several SQL scripts must be executed for Microsoft SQL Server databases.

### Completing the upgrade from Process Engine 3.5 (Oracle):

Complete the upgrade by initiating an automatic schema change in the database.

**Important:** Throughout this procedure there are multiple software restarts. Run all restarts as documented. Do not start or restart Process Task Manager or other IBM FileNet software unless specifically instructed to do so in the procedures. When you restart Process Task Manager it accesses the database, which must not be done until the database has been upgraded.

To run steps on a UNIX operating system, the terminal must support X Window Systems and the DISPLAY environment variable must be set.

To update the Process Engine database objects:

1. After you update the Process Engine software, log onto the Process Engine server.

Option	Description
UNIX	Log on as fnsw.
Windows	Log on as a local administrator.

2. (Windows only) Ensure that the following Process Engine services are started:
  - IMS ControlService
  - Process Engine Services Manager
3. Restart the Process Engine software by entering the following command:  
`initfnsw -y restart`
4. Initiate the database Process Engine schema changes by executing the following command:  
`vwtool`

and then complete the following substeps:

- a. Choose **Yes** when a message is presented indicating that an upgrade is required.
- b. Turn on tracing when prompted as to whether you want to initiate tracing to capture the changes made to a file. Accept the defaults to trace database access and transfer.

**Important:** A number of messages will scroll to the window. Do not choose X in response to the prompt as this will terminate the current **vwtool** command and return an error.

- c. Type exit to end vwtool when the upgrade is complete.

When vwtool starts, it automatically checks the Process Engine database level and updates the schema accordingly.

**Important:** If the upgrade fails at this point, you must restore the Process Engine database backup.

See the Image Services error log to monitor the progress of the updates and ensure that no errors occur. Check the logs to verify that messages like the following examples are captured:

```
2009/10/17 16:23:43.261 <fnsw> VW/Process (14952) ...
[INFO] VW: Database upgrade successful to version 46,
please follow instructions to perform the next step.
```

```
2009/10/17 16:23:43.303 <fnsw> VW/Process (14952) ...
[INFO] VW: Must restart software to complete upgrade procedure
Please follow the upgrade documentation to continue with the upgrade
procedures.
```

You must:

1. Restart the Process Engine software.
2. Configure the Process Engine connection to the Content Engine.
3. Run vwtool to continue the upgrade procedure.

Ignore messages designated as SERIOUS if they are in combination with a successful message for that upgrade, especially if all process IDs are the same for all the errors and INFO messages.

5. Exit vwtool when you get a message that the procedure is complete.
6. Back up the Process Engine database. This backup can serve as a checkpoint if an error occurs later that requires you to restore the database.
7. Restart the Process Engine software. At a Windows command prompt or UNIX command line, enter the following command: `initfnsw -y restart`.

### Completing the upgrade from Process Engine 3.5 (DB2):

The format of the event log files changed. As a part of this upgrade, several SQL scripts must be executed for DB2 databases.

**Important:** Throughout this procedure there are multiple software restarts. Run all restarts as documented. Do not start or restart Process Task Manager or other IBM FileNet software unless specifically instructed to do so in the procedures. When you restart Process Task Manager it accesses the database, which must not be done until the database has been upgraded.

To run steps on a UNIX operating system, the terminal must support X Window Systems and the DISPLAY environment variable must be set.

To update the Process Engine database objects:

1. After you update the Process Engine software, log onto the Process Engine server.

Option	Description
UNIX	Log on as fnsw.
Windows	Log on as a local administrator.

2. (Windows only) Ensure that the following Process Engine services are started:
  - IMS ControlService

- Process Engine Services Manager
3. Edit and run the `\fnsw\DB2\vldb2_35to40_pre1.bat` file on Windows or `\fnsw\DB2\vldb2_35to40_pre1.sh` on UNIX platforms. Database schema changes will be made to `vwnotify` and `vwpending` database tables.
    - a. Save a copy of the file to the same directory, naming it or `vldb2_35to40_pre1a.sh`.
    - b. Change the values in the file as appropriate for your system to:
 

```
db2 connect to database_name user PE_runtime_user using password
```

 where:
      - database\_name* is your Process Engine DB2 database name
      - PE\_runtime\_user* is the Process Engine runtime user (`f_sw`)
      - password* is the Process Engine runtime user password in the Process Engine database
    - c. Run the `vldb2_35to40_pre1a.bat` under from the DB2 command line processor on Windows, or run `vldb2_35to40_pre1a.sh` from a command prompt on UNIX.
  4. Restart the Process Engine software by entering the following command:
 

```
initfnsw -y restart
```
  5. Initiate the database Process Engine schema changes by executing the following command:
 

```
vwtool
```

and then complete the following substeps:

- a. Choose **Yes** when a message is presented indicating that an upgrade is required.
- b. Turn on tracing when prompted as to whether you want to initiate tracing to capture the changes made to a file. Accept the defaults to trace database access and transfer.

**Important:** A number of messages will scroll to the window. Do not choose X in response to the prompt as this will terminate the current **vwtool** command and return an error.

- c. Type exit to end `vwtool` when the upgrade is complete.

When `vwtool` starts, it automatically checks the Process Engine database level, updates the schema accordingly, and creates two additional scripts:

```
fnsw\DB2\vldb2_35to40_post1.sql
fnsw\DB2\vldb2_35to40_post2.sql
```

**Important:** If the upgrade fails at this point, you must restore the Process Engine database backup.

See the Image Services error log to monitor the progress of the updates and ensure that no errors occur. Check the logs to verify that messages like the following examples are captured:

```
2009/10/17 16:23:43.261 <fnsw> VW/Process (14952) ...
[INFO] VW: Database upgrade successful to version 46,
please follow instructions to perform the next step.
```

```
2009/10/17 16:23:43.303 <fnsw> VW/Process (14952) ...
[INFO] VW: Must restart software to complete upgrade procedure
Please follow the upgrade documentation to continue with the upgrade
procedures.
```

You must:

1. Restart the Process Engine software.

2. Configure the Process Engine connection to the Content Engine.
3. Run vwtool to continue the upgrade procedure.

Ignore messages designated as SERIOUS if they are in combination with a successful message for that upgrade, especially if all process IDs are the same for all the errors and INFO messages.

6. Exit vwtool when you get a message that the procedure is complete.
7. Back up the Process Engine database. This backup can serve as a checkpoint if an error occurs later that requires you to restore the database.
8. Restart the Process Engine software. At a Windows command prompt or UNIX command line, enter the following command: `initfnsw -y restart`.

### Completing the upgrade from Process Engine 3.5 (SQL Server):

The format of the event log files have changed. As a part of this upgrade, several SQL scripts must be executed for Microsoft SQL Server databases.

**Important:** Throughout this procedure there are multiple software restarts. Run all restarts as documented. Do not start or restart Process Task Manager or other IBM FileNet software unless specifically instructed to do so in the procedures. When you restart Process Task Manager it accesses the database, which must not be done until the database has been upgraded.

To run steps on a UNIX operating system, the terminal must support X Window Systems and the DISPLAY environment variable must be set.

SQL Server Client software is required on the Process Engine server to run a number of the documented SQL scripts if the database is a remote SQL Server. The SQL Server Client software can be removed from the Process Engine server after the Process Engine database has been successfully upgraded to the 4.5 or later release.

To update the Process Engine database objects:

1. After you update the Process Engine software, log onto the Process Engine server.

Option	Description
UNIX	Log on as fnsw.
Windows	Log on as a local administrator.

2. (Windows only) Ensure that the following Process Engine services are started:
  - IMS ControlService
  - Process Engine Services Manager
3. Edit and run the `\fnsw\mssql\vwssql35to40_pre1.bat` file. Database schema changes will be made to vwnotify and vwpending database tables.
  - a. Save a copy of the file to the same directory, naming it `vwssql35to40_pre1a.bat`.
  - b. Change the values in the file as appropriate for your system. The content of the file looks like this:

```
osql /D DSN /U sa /P sa /n /d instance_name/VWdb /h-1
/i vwssql35to40_pre1.sql /o pre1a.log
```

where:

/D indicates the following variable is your ODBC data source name (DSN). This parameter is not needed if the scripts are running on the database server.

/d indicates the instance and database name. This parameter is not needed if the scripts are run remotely using the DNS name.

/U indicates the following variable is the administrator user name in the Process Engine database.

/P indicates the following variable is the administrator user's password in the Process Engine database.

/d indicates the following variable is the Process Engine database name. Include the *instance\_name* if the database is not in the default instance.

Optionally, you can add an output file /o pre1a.log . Otherwise, all output goes only to the screen.

- c. Run the `vwssql35to40_pre1a.bat` file.
4. Restart the Process Engine software by entering the following command:  
`initfnsw -y restart`
5. Initiate the database Process Engine schema changes by executing the following command:  
`vwtool`

and then complete the following substeps:

- a. Choose **Yes** when a message is presented indicating that an upgrade is required.
- b. Turn on tracing when prompted as to whether you want to initiate tracing to capture the changes made to a file. Accept the defaults to trace database access and transfer.

**Important:** A number of messages will scroll to the window. Do not choose X in response to the prompt as this will terminate the current **vwtool** command and return an error.

- c. Type `exit` to end `vwtool` when the upgrade is complete.

When `vwtool` starts, it automatically checks the Process Engine database level, updates the schema accordingly, and creates two additional scripts:

```
fnsw\mssql\vwssql35to40_post1.sql
fnsw\mssql\vwssql35to40_post2.sql
```

**Important:** If the upgrade fails at this point, you must restore the Process Engine database backup.

See the Image Services error log to monitor the progress of the updates and ensure that no errors occur. Check the logs to verify that messages like the following examples are captured:

```
2009/10/17 16:23:43.261 <fnsw> VW/Process (14952) ...
[INFO] VW: Database upgrade successful to version 46,
please follow instructions to perform the next step.
```

```
2009/10/17 16:23:43.303 <fnsw> VW/Process (14952) ...
[INFO] VW: Must restart software to complete upgrade procedure
Please follow the upgrade documentation to continue with the upgrade
procedures.
```

You must:

1. Restart the Process Engine software.
2. Configure the Process Engine connection to the Content Engine.
3. Run `vwtool` to continue the upgrade procedure.



Ignore messages designated as SERIOUS if they are in combination with a successful message for that upgrade, especially if all process IDs are the same for all the errors and INFO messages.

6. Exit vwtool when you get a message that the procedure is complete.
7. Back up the Process Engine database. This backup can serve as a checkpoint if an error occurs later that requires you to restore the database.
8. Restart the Process Engine software. At a Windows command prompt or UNIX command line, enter the following command: `initfnsw -y restart`.

## Removing existing routers in Process Task Manager

The Process Routers displayed in Process Task Manager are not used and have no effect on the system other than to cause a warning message on Process Task Manager startup.

1. On the Process Engine and Application Engine servers, use Process Task Manager to view, and make note of, the general properties of each Process Router:

- Process Router name
- Process Engine
- Isolated region

2. Delete each Process Router, as follows.

You can do this immediately or wait until the corresponding connection points are created. On a Process Engine that is installed on the same server with an Application Engine, the routers cannot be removed until after the Application Engine and Process Engine client files have been upgraded. After all Process Routers have been deleted and Process Task Manager has been restarted, the Process Router node no longer appears.

- a. Select the Process Router you want to delete.
- b. Select Delete from the Action menu.
- c. Repeat this procedure until you have deleted all Process Routers.

## Updating the Process Engine security

Update the Process Engine security by using the `vwtaskman` tool.

Before you update the Process Engine security, ensure the following is true:

- Your directory server is running and correctly configured.
- Content Engine 4.5 is running.
- You have the CE\_Operations custom settings saved in “Updating all isolated regions” on page 393.

When the Process Task Manager starts, a message is displayed that indicates that routers must be migrated. Routers will be migrated in a subsequent task. The message can be ignored now.

1. Update the information on the Process Task Manager **Security / General** tab, as follows:
  - a. Start Process Task Manager as follows, depending on your operating system:

### Windows

Select **Start** → **Programs** → **IBM FileNet P8 Platform** → **Process Engine** → **Process Task Manager** .

### UNIX

Enter the following command on the command line: `vwtaskman`

- b. Verify that Process Engine is running. To start it, right-click your Process Engine server in the feature pane and choose **Start** from the Action menu.
- c. Select the Process Engine in the feature pane and select the **Security** tab to configure the General settings.

Provide the `pe_service_user` and password, the `pe_admin_group` and the optional `pe_config_group`. The service user name should be entered as a short name, not a distinguished name. See the IBM FileNet P8 help topic **System Administration** → **Enterprise-wide Administration** → **Process Task Manager** → **Process Engine** → **Configure the Process Engine** → **Security** for details on the user and groups.

- d. Click **Apply**. If you get an error applying security settings, click **Close** on the message, correct the problem if noted, and start this procedure again.

Additional information is available in:

#### Windows

```
\fnsw_loc\logs\TM_daemon\PEDirectoryServerConnectionDebug.txt
```

```
UNIX /fnsw/local/logs/TM_daemon/
PEDirectoryServerConnectionDebug.txt
```

- e. Click **OK** to close the dialog box indicating that you must run `vwtool`.
  - f. Exit Process Task Manager.
2. Run `vwtool` and choose **Yes** when a message is presented indicating that an upgrade is required.

This step moves all existing user environment records from the 3.5 format to the 4.5 format.

- a. Enable tracing when prompted.
- b. As user environment records are moved, information is logged to the Image Services error log. When `vwtool` finishes, it will display messages on the screen indicating whether or not the migration was successful, how many users were migrated, and how many users were not migrated. Monitor that log by executing:

```
vl -t
```

- c. Address any errors that occurred run **vwtool** again. You might be prompted to ignore issues related to the user environment record upgrades. If all users did not successfully migrate to the 4.5 format, look at the messages in the error log and resolve the problems. Examples of the types of resolution required could include fixing a problem with the configuration of the Content Engine and its application server's access to the directory server or creating users in the underlying directory server itself.

**Important:** Always choose No in response to the question to override until you have carefully evaluated all users who's environment records did not migrate properly. If you are certain that all unmigrated users are no longer valid Process Engine users, that is, they have no Process Engine work, then you can override these errors and complete this part of the upgrade. If you choose to override these errors, there is no way to recover the user environment records for any users not migrated to 4.5. Any Process Engine work for unmigrated users is lost. Choose **Yes** to ignore errors and force the completion of the upgrade only after you have resolved any outstanding problems.

If **vwtool** fails with a shared memory error, configure contiguous free memory for Process Engine and try again.

3. Check the error log to verify that the database version number has been updated to 55. This update will happen only after either successful migration of all environment records or all errors have been intentionally overridden.
4. At a Windows command prompt, or UNIX command line, type the following to restart the Process Engine software:  

```
initfnsw -y restart
```
5. This restart of the software starts an automatic transfer of the `upgrade.cdl` file for all isolated regions. Monitor the syslogs for progress by executing:  

```
vl -t
```

If messages in the log indicate that any isolated region failed for phase 2 of the upgrade, the isolated region will be locked and the upgrade will proceed for other isolated regions. Make note of any region numbers where this phase of the upgrade failed.

6. Run the following substeps for any isolated region where the transfer failed.
  - a. Start `vwtool` and enter the following at the prompt:  

```
reg XXX
```

where:  
XXX indicates a region where the automatic transfer failed
  - b. Enter at the `vwtool` prompt:  

```
unlockreg
```
  - c. Repeat the unlock for every region that failed.
  - d. Change directories to the following location of the `upgrade.cdl` file, depending on your operating system:

**Windows**

```
\fnsw_loc\sd
```

**UNIX** /fnsw/local/sd

- e. Initiate a transfer on isolated regions that failed the automatic upgrade by entering the following command:  

```
wtfer -o upgrade.cdl -r XXX
```

where:  
-r XXX indicates a region where the automatic transfer failed  
At the prompt, log on as `pe_service_user`.
- f. Repeat the transfer on every region that failed.
- g. Restore the custom settings for CE\_Operations saved before the upgrade in “Updating all isolated regions” on page 393.

### Running post-upgrade scripts Microsoft SQL Server and DB2

Run two post-upgrade scripts. For each database type, the first script copies records from archived event-log tables to the new 4.5 version of the tables, and the second script deletes the archived log tables, thereby saving database space.

“Running post-upgrade scripts (Microsoft SQL Server)” on page 430

Run these scripts to copy records from archived event-log tables to a new version of the tables, and delete the archived log tables, thereby saving database space.

“Running post-upgrade scripts (DB2)” on page 431

Run these scripts to copy records from archived event-log tables to a new version of the tables, and delete the archived log tables, thereby saving database space.

## Running post-upgrade scripts (Microsoft SQL Server):

Run these scripts to copy records from archived event-log tables to a new version of the tables, and delete the archived log tables, thereby saving database space.

The `vmssql35to40_post1.bat` script copies the event-log tables to the new version and the `vmssql35to40_post2.bat` script deletes the archived log tables. The second script is optional. Do not run the second script until you verify that the first script ran with no errors.

1. Edit and run the `\fnsw\mssql\vmssql35to40_post1.bat` file, as follows:
  - a. Save the `vmssql35to40_post1.bat` file to the same directory, naming it `vmssql35to40_post1a.bat`.
  - b. Change the values in the `vmssql35to40_post1a.bat` file as appropriate for your system. The contents of the file look like this:

```
osql /D DSN /U sa /P sa /n /d instance_name/VWdb /h-1
/i vmssql35to40_post1.sql /o post1a.log
```

where:

`/D` indicates the following variable is your ODBC data source name (DSN). This parameter is not needed if the scripts are running on the database server.

`/d` indicates the instance and database name. This parameter is not needed if the scripts are run remotely using the DNS name.

`/U` indicates the following variable is the administrator user name in the Process Engine database.

`/P` indicates the following variable is the administrator user's password in the Process Engine database.

`/d` indicates the following variable is the Process Engine database name. Include the `instance_name` if the database is not in the default instance.

`/o` indicates the following variable is the optional `post1a.log` output file. If you choose to eliminate this entry, output displays to the screen only.

- c. Run the `vmssql35to40_post1a.bat` file.
2. Delete archived event log tables by editing and running `vmssql35to40_post2.bat`.
  - a. Save the `vmssql35to40_post2.bat` file to the same directory, naming it `vmssql35to40_post2a.bat`.
  - b. Change the values in the `vmssql35to40_post2a.bat` file as appropriate for your system. The contents of the file look like this:

```
osql /D DSN /U sa /P sa /n /d instance_name/VWdb /h-1
/i vmssql35to40_post2.sql /o post2a.log
```

where:

`/D` indicates the following variable is your ODBC data source name (DSN). This parameter is not needed if the scripts are running on the database server.

`/U` indicates the following variable is the administrator user name in the Process Engine database.

`/P` indicates the following variable is the administrator user's password in the Process Engine database.

`/d` indicates the following variable is the Process Engine database name. Include the `instance_name` if the database is not in the default instance.

`/o` indicates the following variable is the optional `post2a.log` output file. If you choose to eliminate this entry, output displays to the screen only.

- c. Run the `vmssql35to40_post2a.bat` file.

### Running post-upgrade scripts (DB2):

Run these scripts to copy records from archived event-log tables to a new version of the tables, and delete the archived log tables, thereby saving database space.

The `vwdb2_35to40_post1.sql` script copies the event-log tables to the new version and the `vwdb2_35to40_post2.sql` script deletes the archived log tables. The second script is optional. Do not run the second script until you verify that the first script ran with no errors.

1. Connect to the DB2 database and run the `\fnsw\DB2\vwdb2_35to40_post1.sql` file.
  - a. Start the DB2 command line processor and log on to the Process Engine database with the Process Engine runtime user (`f_sw`).
  - b. Enter the following command in that window:  
`db2 connect to database_name user PE runtime user using password`  
where:  
`database_name` is your Process Engine DB2 database name.  
`PE runtime user` is the Process Engine runtime user (`f_sw`).  
`password` is the Process Engine runtime user password in the Process Engine database.
  - c. Run the `vwdb2_35to40_post1.sql` file by executing the following in the DB2 command line processor:  
`db2 -tvf vwdb2_35to40_post1.sql`
2. Connect to the DB2 database and run the `\fnsw\DB2\vwddb2_35to40_post2.sql` file, as follows:
  - a. Start the DB2 command-line processor and log on to the Process Engine database with the Process Engine runtime user (`f_sw`),
  - b. Enter the following command in that window:  
`db2 connect to database_name user PE runtime user using password`  
where:  
`database_name` is your Process Engine DB2 database name.  
`PE runtime user` is the Process Engine runtime user (`f_sw`).  
`password` is the Process Engine runtime user password in the Process Engine database.
  - c. Run the `vwddb2_35to40_post2.sql` file by executing the following in the DB2 command-line processor:  
`db2 -tvf vwdb2_35to40_post2.sql`

### Configuring contiguous free memory for Process Engine (Windows)

Use the procedure in this task to enable Process Engine to use the largest available contiguous free memory area for shared memory allocations. Unless you perform this procedure, at some point during normal execution the system will not allocate shared memory and will cease to function correctly.

To configure contiguous free memory for Process Engine:

1. Log on as the `fnsw` (or alias) user.
2. Restart the Process Engine software. At a Windows command prompt, enter:  
`initfnsw -y restart`

3. Find the largest available shared memory block and create an executable file with a .reg file extension. That file will be run to update the registry to create a new DWORD value.
  - a. Create the file by entering the following at a Windows command prompt: `set_shm_address -r shmaddress.reg` where:
    - `-r` indicates an input file
    - `shmaddress.reg` is the name of the file that contains registry information. This file must have the .reg file extension.
  - b. Verify the contents of the output file. The following are examples of the file content.

#### 32-bit Windows

```
[HKEY_LOCAL_MACHINE\SOFTWARE\FileNET\IMS\CurrentVersion]
"StartShmAddress"=dword:12230000
```

#### 64-bit Windows

```
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\FileNET\IMS\CurrentVersion]
"StartShmAddress"=dword:12230000
```

4. Run the executable file to update the registry by typing the following at a Windows command: `shmaddress.reg shmaddress.reg` `shmaddress.reg` is the file you just created.
5. Restart the Process Engine software. At a Windows command prompt, enter: `initfnsw -y restart`
6. Verify the setting that you just applied for the shared memory address by entering the following command at a command prompt: `set_shm_address -v`

### Migrating routers and updating isolated regions

Convert all routers to connection points and assign passwords to any existing isolated regions.

1. "Configuring new regions in IBM FileNet Enterprise Manager"  
You must configure an isolated region for each unique Process Engine / isolated region combination. These new regions replace the routers that were removed in earlier steps in the upgrade.
2. "Configuring new regions in Process Task Manager" on page 433  
Configure new regions by using the Process Task Manager.

#### Configuring new regions in IBM FileNet Enterprise Manager:

You must configure an isolated region for each unique Process Engine / isolated region combination. These new regions replace the routers that were removed in earlier steps in the upgrade.

1. Start Enterprise Manager.
2. Navigate to the Process Engine Region IDs node and start the wizard.
3. Specify an isolated region for each unique Process Engine / isolated region combination. (If you have more than one Process Router pointing to the same Process Engine / isolated region combination, you will identify only one Process Engine Region ID.)

For this Process Engine Region ID property	Use the value from this Process Router property
DNS name or IP address of the Process Engine This is the network name for the Process Engine.	Process Engine
Region number	Isolated region

4. Assign a password for each region as you create it. Make note of the password you assign. You must enter that password in the steps that follow for assigning the password to regions in Process Task Manager. The passwords must match.
5. Navigate to the Process Engine Connection Points node, start the wizard, and create new connection points for each region.
6. Close Enterprise Manager.

### Configuring new regions in Process Task Manager:

Configure new regions by using the Process Task Manager.

1. Start Process Task Manager on the Process Engine server as follows, depending on your operating system:

Option	Description
Windows	Select <b>Start</b> → <b>Programs</b> → <b>IBM FileNet P8 Platform</b> → <b>Process Engine</b> → <b>Process Task Manager</b>
UNIX	Enter the following command on the command line: <code>vwtaskman</code>

(UNIX) The terminal must support X Windows and the DISPLAY environment variable must be set.

2. Select Process Engine in the feature pane.
3. Right-click on the **Regions** folder, select **New** to create a new region.
4. Select the **Security Settings** sub-tab to set a region password. The password you enter here must match the password entered for the region as it is defined in the Enterprise Manager.

After you have entered all parameters, click **Apply** and restart the Process Service when prompted. If errors are returned, additional information is available in the following file:

Option	Description
Windows	<code>\fnsw_loc\logs\TM_daemon\PEDirectoryServerConnectionDebug.txt</code>
UNIX	<code>/fnsw/local/logs/TM_daemon/PEDirectoryServerConnectionDebug.txt</code>

### Updating email notification

Enable email notification in order to use it. Process Engine also supports localized email notification.

1. Add a language pack for the Default Authoring Locale.  
See the IBM FileNet P8 help topic *System Administration > Process Engine Administration > Workflow administration tasks > Coordinating workflow design > Enable Email notification* for information on adding a language pack for the Default Authoring Locale.
2. Verify that the Default Authoring Locale is correct (it has defaulted to the operating system's locale).
3. Process Engine supports localized email notification. For details on configuring this, see the *IBM FileNet P8 Non-English Support Guide*.



## Related information



Product documentation for IBM FileNet P8 Platform

Download the IBM FileNet P8 Non-English Support Guide, as well as PDF's of the rest of the IBM FileNet P8 Platform documentation.

## Backing up the database and restarting software

Back up and restart the database software after upgrading.

1. Back up the Process Engine database. While this backup is not required, it is a best practice. It provides a checkpoint that can be used later if a restore is needed in the context of this upgrade.
2. (Windows only) Start the following services and set them back to automatic startup.
  - IMS ControlService
  - Process Engine Services Manager
3. Restart the Process Engine software, as follows:  
At a Windows command prompt, or UNIX command line, type the following command:  
`initfnsw -y restart`

## Completing the upgrade from Process Engine 4.0, 4.5.0, or higher

Perform the following steps to update a Process Engine database to version 4.5.1. A database update will take place automatically by restarting the software.

Before starting this procedure, ensure you have the CE\_Operations custom settings saved in "Updating all isolated regions" on page 398. To update the database to version 4.5.1:

1. Run the following command to restart the Process Engine:  
`initfnsw -y restart`
2. Monitor the syslogs for progress by executing:  
`v1 -t`
3. Verify that messages similar to the following are captured:  

```
2009/07/27 15:47:14.632 <fnsw> VW/Process (3564.2552.12 0xdec.9f8)
... [INFO]VW (vwcomp):
Database upgrade successful to version 55
2009/07/27 15:47:14.679 <fnsw> VW/Process (3564.2552.12 0xdec.9f8)
... [INFO]VW (vwcomp):
Create report 'C:\FNSW_LOC\logs\peconfig\dbUpgradeRpt_55_20090727'
2009/07/27 15:47:17.240 <fnsw> VW/Process (3564.2552.12 0xdec.9f8)
... [INFO]VW (vwcomp):
Completed report 'C:\FNSW_LOC\logs\peconfig\dbUpgradeRpt_55_20090727'
2009/07/27 15:47:17.256 <fnsw> VW/Process (3564.2552.12 0xdec.9f8)
...VW (vwcomp):
Completed phase 1 upgrade
```
4. Continue to monitor the syslogs for progress by executing:  
`v1 -t`

The software will automatically be restarted again to complete phase 2 of the upgrade process. The automatic restart of the software occurs in the background and will not be reflected in the command window. If the software cannot be restarted, messages will be logged. Manually restart the software if the automatic restart fails.

5. This restart of the software starts an automatic transfer of the upgrade.cdl file for all isolated regions. Monitor the syslogs for progress by executing:
 

```
v1 -t
```

6. Verify that messages similar to the following are captured:
 

```
2009/07/27 15:48:30.488 <fns> VW/Process (2040.3388.10 0x7f8.d3c)
... [INFO]VW (vwcomp):
PE upgrade phase 2 completed.
2009/07/27 15:48:30.503 <fns> VW/Process (2040.3388.10 0x7f8.d3c)
... [INFO]VW (vwcomp):
Enable PE daemon processes
2009/07/27 15:48:30.519 <fns> VW/Process (2040.3388.10 0x7f8.d3c)
... [INFO]VW (vwcomp):
Start PE daemon processes ...
```

If messages in the log indicate that any isolated region failed for phase 2 of the upgrade, the isolated region will be locked and the upgrade will proceed for other isolated regions. Make note of any region numbers where this phase of the upgrade failed.

7. Complete the following substeps for any isolated region where the transfer failed.
  - a. Start vwtool and enter the following at the prompt:
 

```
reg XXX
```

 where:
 

XXX indicates a region where the automatic transfer failed
  - b. Enter at the vwtool prompt:
 

```
unlockreg
```
  - c. Repeat the unlock for every region that failed.
  - d. Change directories to the following location of the *upgrade.cdl* file, depending on your operating system:

**Windows**

```
\fnsw_loc\sd
```

**UNIX** /fnsw/local/sd

- e. Initiate a transfer on isolated regions that failed the automatic upgrade by entering the following command:
 

```
wtfer -o upgrade.cdl -r XXX
```

 where:
 

-r XXX indicates a region where the automatic transfer failed

At the prompt, log on as *pe\_service\_user*.
  - f. Repeat the transfer on every region that failed.
  - g. Restore the custom settings for CE\_Operations saved before the upgrade in "Updating all isolated regions" on page 398.
1. "Configuring contiguous free memory for Process Engine (Windows)" on page 436
 

Use the procedure in this task to enable Process Engine to use the largest available contiguous free memory area for shared memory allocations. Unless you perform this procedure, at some point during normal execution the system will not allocate shared memory and will cease to function correctly.
2. "Backing up the database and restarting software" on page 436
 

Back up and restart the database software after upgrading.

## Configuring contiguous free memory for Process Engine (Windows)

Use the procedure in this task to enable Process Engine to use the largest available contiguous free memory area for shared memory allocations. Unless you perform this procedure, at some point during normal execution the system will not allocate shared memory and will cease to function correctly.

To configure contiguous free memory for Process Engine:

1. Log on as the `fns` (or alias) user.
2. Restart the Process Engine software. At a Windows command prompt, enter:  
`initfns -y restart`
3. Find the largest available shared memory block and create an executable file with a `.reg` file extension. That file will be run to update the registry to create a new `DWORD` value.
  - a. Create the file by entering the following at a Windows command prompt:  
`set_shm_address -r shmaddress.reg` where:
    - `-r` indicates an input file
    - `shmaddress.reg` is the name of the file that contains registry information. This file must have the `.reg` file extension.
  - b. Verify the contents of the output file. The following are examples of the file content.

### 32-bit Windows

```
[HKEY_LOCAL_MACHINE\SOFTWARE\FileNET\IMS\CurrentVersion]
"StartShmAddress"=dword:12230000
```

### 64-bit Windows

```
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\FileNET\IMS\CurrentVersion]
"StartShmAddress"=dword:12230000
```

4. Run the executable file to update the registry by typing the following at a Windows command: `shmaddress.reg` `shmaddress.reg` is the file you just created.
5. Restart the Process Engine software. At a Windows command prompt, enter:  
`initfns -y restart`
6. Verify the setting that you just applied for the shared memory address by entering the following command at a command prompt: `set_shm_address -v`

## Backing up the database and restarting software

Back up and restart the database software after upgrading.

1. Back up the Process Engine database. While this backup is not required, it is a best practice. It provides a checkpoint that can be used later if a restore is needed in the context of this upgrade.
2. (Windows only) Start the following services and set them back to automatic startup.
  - IMS ControlService
  - Process Engine Services Manager
3. Restart the Process Engine software, as follows:  
At a Windows command prompt, or UNIX command line, type the following command:  
`initfns -y restart`

---

## Installing Process Engine software updates

After installing Process Engine, software updates such as fix packs or interim fixes might also be required.

If you installed an instance into a high availability environment, perform the procedure on every node.

To install the Process Engine software updates:

1. To obtain the latest Process Engine software updates, and to determine whether additional interim fixes are needed, contact your service representative.
2. Open the readme files for the Process Engine software updates and perform the installation procedures in the readme files on the Process Engine.

---

## Installing the latest Process Engine client files on other IBM FileNet P8 servers (for staged upgrades)

When you upgrade Process Engine server software, you must also upgrade the associated Process Engine Client files installed on other machines running FileNet P8 components, for example, on Content Engine and Application Engine servers.

In a standard upgrade of your FileNet P8 system, you would install these client files in the course of upgrading each respective component.

However, if you are staging your FileNet P8 upgrade over a period of time and not upgrading one or more of the other FileNet P8 components at this time, you must still perform the Process Engine Client install on the other component machines.

- You will have this same client-installation requirement for any expansion products that use Process Engine Client files, such as:
  - IBM FileNet Workplace XT
  - IBM InfoSphere Enterprise Records
  - IBM FileNet Business Process Framework
- You must redeploy any components that are web-application-server based, such as Content Engine, Application Engine, Workplace XT, and FileNet Records Manager after you upgrade the Process Engine Client files on the associated machines.



---

## Upgrading and configuring Application Engine

You can upgrade Application Engine from version 3.5 or version 4.0 to version 4.0.2. The procedures for upgrading Application Engine vary depending on the version that you are upgrading.

**Important:** Before you start to upgrade the Application Engine software, ensure that you are at the correct version and fix pack level, as indicated in *Plan and Prepare Your Environment for IBM FileNet P8*.

1. "Preparing for Application Engine upgrade" on page 440  
Before you upgrade your Application Engine installation, you must prepare your existing configuration for the upgrade. This preparation includes backing up existing files and undeploying your web application.
2. "Upgrading Application Engine" on page 443  
After you have prepared your existing configuration, you can begin the Application Engine upgrade. The tasks for upgrading Application Engine differ depending on whether you start from version 3.5 or version 4.0.
3. "Installing Application Engine software updates" on page 448  
If any required fix packs and interim fixes exist for Application Engine, you must install these software updates.
4. "Installing the latest Content Engine client files on Application Engine servers" on page 449  
The Content Engine Client software enables communication between the Application Engine and the Content Engine. Install the latest release or fix pack version of the Content Engine Client files on all Application Engine servers.
5. "Installing the latest Process Engine client files on Application Engine servers" on page 454  
The Process Engine Client software enables communication between the Application Engine and the Process Engine. You must install the Process Engine Client files on all Application Engine servers.
6. "Configuring Application Engine upgrades from 3.5" on page 457  
After you complete the Application Engine upgrade from 3.5, you must configure Application Engine files and your application sever to enable communication between Application Engine and Content Engine. You can choose the appropriate configuration tasks for your application server type and environment.
7. "Manually copying custom data" on page 478  
If your custom data was not retained in the upgrade, you must manually copy the data from the version 3.5 or 4.0.1 backup files (deploy\_backup) to the upgraded directories.
8. "Deploying upgraded instances of Application Engine" on page 478  
After you upgrade and configure Application Engine, deploy your client application, Workplace, on your application server. It might be necessary to re-create the WAR or WAR and EAR files before you deploy.
9. "Completing post-upgrade Application Engine configuration" on page 486  
After you upgrade and deploy your Application Engine instances, you can complete additional configuration. Actions include modifying a configuration file, verifying Workplace sign-in, and establishing the Process Engine connection point.

## Related information

 General requirements for all FileNet P8 Platform systems  
Check to make sure your software is at the correct fix pack level before you upgrade.

---

## Preparing for Application Engine upgrade

Before you upgrade your Application Engine installation, you must prepare your existing configuration for the upgrade. This preparation includes backing up existing files and undeploying your web application.

- (Upgrades from 3.5 only) Verify that Content Engine and Process Engine have been upgraded.
- Review the Application Engine details of the guide *Plan and Prepare Your Environment for IBM FileNet P8*.
- Review the steps needed to retain the Application Engine 3.5 or 4.0.1 configuration. You will need this information if, for any reason, you want to back out of this installation.
- Verify that you have recorded all necessary settings.

(Best practices for backup) If you want to retain your existing Application Engine settings you must record all necessary settings before you start the upgrade installation.

- As part of the upgrade you will create backup copies of all important 3.5 or 4.0.1 configuration files.
  - During the upgrade, a number of existing configuration files will be moved to the newly created *AE\_install\_path/Config/AE* directory.
  - As part of the upgrade, the installation program automatically creates a backup of your existing Application Engine 3.5 or 4.0.1 configuration files, appending the suffix *.old* to the file names.
  - The existing version 3.5 or 4.0.1 *Actions.xml* and *web.xml* files will be merged with the 4.0.2 versions during the upgrade.
  - In addition, all comments added to the *Actions.xml* file will be lost during the merge.
- If you have the IBM FileNet P8 eForms expansion product installed, uninstall it.

See the "Removing Software" topic in the *IBM FileNet P8 eForms Installation and Upgrade Guide*.

To prepare for the Application Engine upgrade:

1. Log on to the Application Engine server:

Option	Description
UNIX	Log on as a user with read, write, and execute access to the directory where you plan to install Application Engine.
Windows	Log on as a member of the local Administrators group or a user with equivalent permissions.

2. (Upgrades from 3.5 only) Verify that the Process Router is stopped.



**Tip:** Although the Application Engine router has been deleted as part of the Process Engine upgrade, a local, disconnected instance might be running on your server.

- a. Launch the Process Task Manager from `AE_install_path/Router` :

**UNIX** `./routercmd.sh`

**Windows**

`routercmd.bat`

- b. Stop the router, if running.

This is the router configured and started as part of the FileNet P8 Platform 3.5 installation. For more information, see the *IBM FileNet P8 Platform 3.5 Installation and Upgrade Guide* task "Start the Process Router."

- c. Exit the Process Task Manager.

3. (Windows) Using the Windows Task Manager, verify that no `javaw.exe` processes are running. If the applications in the preceding steps stopped correctly, no Application Engine related `javaw.exe` processes should be running.

- a. Use Windows Services to stop the Process Application Engine Services Manager Service. Select **Start** → **Programs** → **Administrative Tools** → **Services**. If the Process Application Engine Services Manager status is started, right-click the item and click **Stop**.

- b. If there are still `javaw.exe` processes running after stopping the Process Application Engine Services Manager, use the Windows Task Manager to stop any Application Engine related `javaw.exe` processes.

4. Back up, undeploy, and remove the Workplace Web application from the J2EE application server.

During this step you will create a backup copy of the deployed Web application containing all customized files and all configuration files stored in the `WEB-INF` directory.

Even though the installer automatically creates a backup of your existing Application Engine 3.5 or 4.0.1 configuration files, it is a best practice to back up the following directories to get a complete backup of your deployed system. You might need these files in later steps to retain your 3.5 or 4.0.1 settings. For example, when you copy modified files to the installed Workplace directory and perform the upgrade and configuration of Application Engine,

Option	Description
WebSphere Application Server	<ol style="list-style-type: none"> <li>1. Make a backup copy of the deployed Workplace directory (<i>deploy_backup</i>):  <code>WAS_HOME/profiles/default/installedApps/node_name/app_engine_war.ear/app_engine.war</code>            Your path might vary if you created a new profile or renamed your WAR file.</li> <li>2. Stop the Workplace application from the WebSphere administrative console.</li> <li>3. Uninstall the Workplace application from <b>Enterprise Applications</b>.</li> <li>4. Save the changes and stop the WebSphere Application Server.</li> <li>5. Delete the temp Workplace directory (default: <i>app_engine_war</i>) from:  <code>WAS_HOME/profiles/default/temp/node_name/instance/app_engine.war</code></li> </ol>

Option	Description
<b>WebLogic Server</b>	<ol style="list-style-type: none"> <li>1. From the WebLogic Server Administration Console, stop the Workplace web application module.</li> <li>2. Make a backup copy of the Workplace folder (<i>deploy_backup</i>): <i>AE_install_path</i>/Workplace</li> <li>3. Delete the Workplace Web Application Module.</li> <li>4. Stop the WebLogic Server.</li> </ol>
<b>JBoss Application Server</b>	<ol style="list-style-type: none"> <li>1. Stop the JBoss Application Server.</li> <li>2. Make a backup copy of the deployed Workplace directory (<i>deploy_backup</i>): <i>JBoss_HOME</i>/server/default/deploy/Workplace.war</li> <li>3. Delete the deployed Workplace directory: <i>JBoss_HOME</i>/server/default/deploy/Workplace.war</li> <li>4. Delete the temporary Workplace directory for JBoss: <i>JBoss_HOME</i>/server/default/work/jboss.web/localhost/Workplace</li> </ol>

5. Copy modified files to the installed Workplace directory. During the upgrade, the configuration files will be moved from the following directory:

*AE\_install\_path*/Workplace/WEB-INF to  
*AE\_install\_path*/Config/AE

If you have made modifications to any of these files directly in the deployed Workplace directory (app\_engine.war for WebSphere Application Server or Workplace.war for JBoss) in your 3.5. or 4.0.1 environment, you must copy the modified version of these files from the *deploy\_backup* directory to the installed directory *AE\_install\_path*/Workplace/WEB-INF before you run the installer.

- actions.xml
- bootstrap.properties
- ClassFilter.xml
- ConfigurableLabels.xml
- containericons.properties
- content\_redir.properties
- customobjecticons.properties
- download\_redir.properties
- fnsoap.xml
- icons.properties
- InfoPages.xml
- PagingConfiguration.xml
- PolicyProcessors.xml
- PrimaryViews.xml
- PropertiesPages.xml
- SimpleSearch.xml
- SystemsPropertiesView.xml

As part of the upgrade the installation program automatically creates a backup of your existing Application Engine 3.5 or 4.0.1 configuration files, appending the suffix .old to the file names.

- actions.xml.old
- ClassFilter.xml.old
- ConfigurableLabels.xml.old
- containericons.properties.old
- content\_redir.properties.old
- icons.properties.old
- SystemsPropertiesView.xml.old
- UpdateActions.xml.old
- UpdateClassFilter.xml.old
- UpdateConfigurableLabels.xml.old
- UpdateProps.xml.old
- UpdateSystemPropertiesView.xml.old
- UpdateWeb.xml.old
- web.xml.old

The backed up files are located in: *AE\_install\_path/backup-4\_0\_2*

#### Related tasks

“Manually copying custom data” on page 478

If your custom data was not retained in the upgrade, you must manually copy the data from the version 3.5 or 4.0.1 backup files (deploy\_backup) to the upgraded directories.

---

## Upgrading Application Engine

After you have prepared your existing configuration, you can begin the Application Engine upgrade. The tasks for upgrading Application Engine differ depending on whether you start from version 3.5 or version 4.0.

#### “Upgrading Application Engine from 3.5”

An upgrade from version 3.5 resembles a new install. You can choose to upgrade Application Engine interactively by using the upgrade wizard, or silently by using a silent input file.

#### “Upgrading Application Engine from 4.0” on page 446

In an upgrade from version 4.0 or later, the upgrade tool verifies that the currently installed version of Application Engine can be upgraded. You can choose to upgrade Application Engine interactively by using the upgrade wizard, or silently by using a silent input file.

## Upgrading Application Engine from 3.5

An upgrade from version 3.5 resembles a new install. You can choose to upgrade Application Engine interactively by using the upgrade wizard, or silently by using a silent input file.

- 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. For details, see “Deploying multiple Application Engine instances” on page 189.

- Before logging on to Workplace for the first time, at least one object store must exist on the Content Engine to hold the site preferences. See “Creating the initial object store” on page 76 for more information.
- You can install a new Application Engine 4.0.2 server within an existing 4.0 IBM FileNet P8 environment if your Content Engine is at version 401.006 or later and your Process Engine is at 403-000.001 or later. The Content Engine and Process Engine client files you install on the Application Engine must match the version of your Content Engine and Process Engine.

“Upgrading Application Engine interactively”

You can use the installation wizard to upgrade Application Engine. To complete the upgrade, provide the necessary parameter values to enable the Application Engine client application, Workplace to access the information that is managed by Content Engine.

“Upgrading Application Engine silently” on page 445

You can include the parameters for your Application Engine upgrade in a silent input file, and then run the upgrade from a command line.

### Upgrading Application Engine interactively

You can use the installation wizard to upgrade Application Engine. To complete the upgrade, 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.

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. Log on to the application server.

Option	Description
UNIX	Log on as a user with read, write, and execute access to the directory where you plan to install Application Engine.
Windows	Log on as a member of the local Administrators group or a user with equivalent permissions.

3. Access the IBM FileNet P8 Application Engine 4.0.2.0 installation software.


4. Start the installation program.

Platform	Command
AIX	P8AE-4.0.2.0-AIX.bin
HPUX	P8AE-4.0.2.0-HPUX.bin
HPUXi	P8AE-4.0.2.0-HPUX64.bin
Linux	P8AE-4.0.2.0-LINUX.bin
Solaris	P8AE-4.0.2.0-SOL.bin
Windows	P8AE-4.0.2.0-WIN.exe

Platform	Command
Linux on System z	P8AE-4.0.2.0-ZLINUX.bin

- Complete the Application Engine installer screens by using the values from your worksheet.
- 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.

### 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*.

## Upgrading Application Engine silently

You can include the parameters for your Application Engine upgrade in a silent input file, and then run the upgrade from a command line.

To upgrade the Application Engine software silently:

- Log on to the application server, as appropriate for your operating system:

Option	Description
UNIX	Log on as a user with read, write, and execute access to the directory where you plan to install Application Engine.
Windows	Log on as a member of the local Administrators group or a user with equivalent permissions.

- 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.
- Follow the instructions in the silent input file to edit the file to record the appropriate responses for your installation.
- Modify all instances of `AE_install_path` in the script as follows.

#### UNIX

Change `../FileNet/AE` to `../FileNet`

#### Windows

Change `..\FileNet\AE` to `..\FileNet`

Change `.\FileNet\AE` to `.\FileNet`

- From a command prompt, navigate to and run the installer.

#### UNIX

```
./P8AE-4.0.2.0-operating system.bin -options
path_to_edited_input_file/AE_silent_input.txt -silent
```

#### Windows

```
P8AE-4.0.2.0-Win.exe -options
path_to_edited_input_file\AE_silent_input.txt -silent
```

- 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.

### 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*.

## Upgrading Application Engine from 4.0

In an upgrade from version 4.0 or later, the upgrade tool verifies that the currently installed version of Application Engine can be upgraded. You can choose to upgrade Application Engine interactively by using the upgrade wizard, or silently by using a silent input file.

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

- If you plan to install and use the IBM FileNet Workplace XT product, installing Application Engine is not required.
- To ensure proper functionality and performance, only install one instance of Application Engine per application server (or virtual machine or WebSphere 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 Engine to hold the site preferences.


“Upgrading Application Engine from 4.0 interactively”

You can use the installation wizard to upgrade Application Engine. To complete the upgrade, provide the necessary parameter values to enable the Application Engine client application, Workplace, to access the information that is managed by Content Engine.

“Upgrading Application Engine from 4.0 silently” on page 447

You can include the parameters for your Application Engine upgrade in a silent input file, and then run the upgrade from a command line.

### 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

“Deploying multiple Application Engine instances” on page 189

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.

“Creating the initial object store” on page 76

You create an initial object store in Content Engine to store your documents and other objects. After an object store is created, you can refine its definition and add content to it.

## Upgrading Application Engine from 4.0 interactively

You can use the installation wizard to upgrade Application Engine. To complete the upgrade, provide the necessary parameter values to enable the Application Engine client application, Workplace, to access the information that is managed by Content Engine.

To upgrade Application 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 Application Engine values, filter by **AE Installer** in the **Installation or Configuration Program** column.

2. Log on to the server where Application Engine is installed:

Option	Description
UNIX	Log on as a user with read, write, and execute access to the directory where you plan to install Application Engine.
Windows	Log on as a member of the local Administrators group or a user with equivalent permissions.

Although the installing user must have write access to the /bin directory, the Application Engine installer does not write to that directory.

3. Access the IBM FileNet Application Engine 4.0.2 installation software.
4. Start the installation program.


Platform	Command
AIX	P8AE-4.0.2.0-AIX.bin
HPUX	P8AE-4.0.2.0-HPUX.bin
HPUXi	P8AE-4.0.2.0-HPUX64.bin
Linux	P8AE-4.0.2.0-LINUX.bin
Solaris	P8AE-4.0.2.0-SOL.bin
Windows	P8AE-4.0.2.0-WIN.exe
Linux on System z	P8AE-4.0.2.0-ZLINUX.bin

5. Complete the Application Engine installation program screens by using the values in your worksheet.

In addition to the prompts for system-specific information, you can choose to deploy Application as a WAR file or an EAR file. If you decide to deploy Application Engine as a WAR file and later decide to redeploy as an EAR file you must uninstall Application Engine and then reinstall the application, selecting EAR file deployment.

6. View the `app_engine_install_log_4_0_2.txt` file located, located in `AE_install_path/Logs`. Verify that no errors or failures were logged. Correct any errors before you proceed.

#### 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*.

### Upgrading Application Engine from 4.0 silently

You can include the parameters for your Application Engine upgrade in a silent input file, and then run the upgrade from a command line.

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 Application Engine values, filter by **AE Installer** in the **Installation or Configuration Program** column.

2. Log on to the server where Application Engine is installed:

Option	Description
UNIX	Log on as a user with read, write, and execute access to the directory where you plan to install Application Engine.
Windows	Log on as a member of the local Administrators group or a user with equivalent permissions.

Although the installing user must have write access to the /bin directory, the Application Engine installer does not write to that directory.

3. Edit the silent input file to reflect the appropriate responses for your upgrade by following the instructions in the file and the values in your worksheet.
4. From a command prompt, navigate to the installer and run it.

#### UNIX

```
./P8AE-4.0.2.0-operating system.bin -options
path_to_edited_input_file/AE_silent_input.txt -silent
```


#### Windows

```
P8AE-4.0.2.0-Win.exe -options
path_to_edited_input_file\AE_silent_input.txt -silent
```

5. 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.

#### 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 Application Engine software updates

If any required fix packs and interim fixes exist for Application Engine, you must install these software updates.

To install the Application Engine software updates:

1. To download the latest software updates, and to determine which of these updates might be required for use with other components and expansion products, contact your support representative.
2. Open the readmes for any subsequent fix packs or interim fixes (typically optional) and perform the installation procedures provided.
3. Install the latest updates for the Content Engine Client and Application Engine Client files using the subsequent tasks.

---

## Installing the latest Content Engine client files on Application Engine servers

The Content Engine Client software enables communication between the Application Engine and the Content Engine. Install the latest release or fix pack version of the Content Engine Client files on all Application Engine servers.

**Important:** If you are performing a staged upgrade, and you are upgrading Application Engine before you upgrade Content Engine, it is not necessary to complete this task at this time. When you upgrade Content Engine to version 4.5.1, you must then use this task to run the version 4.5.1 Content Engine Client installer on your Application Engine, and redeploy the Workplace application.

Depending on the Content Engine Client versions that you have installed, you might have more than one instance of the Content Engine Client version 4.0 installed. Additionally, the version 4.0 Content Engine Client installer supported installing multiple instance of the Content Engine Client on the same server. Uninstall all instances before upgrading to Content Engine Client version 4.5.1.

*“Removing the Content Engine 4.0 Client files from Application Engine servers”*  
Before you upgrade the Content Engine Client files to version 4.5.1, you must remove the version 4.0 Client files.

*“Installing the latest Content Engine Client files on Application Engine servers interactively”* on page 451

The installation wizard provides an interactive way to install the Content Engine Client files. You can use the values you collected on your worksheet to fill in the required value for each field on the wizard screens.

*“Installing the Content Engine Client files silently”* on page 452

The command line method provides a way to silently install the Content Engine Client files. You can use the values in your installation worksheet to edit the silent input text file before you run the installation.

## Removing the Content Engine 4.0 Client files from Application Engine servers

Before you upgrade the Content Engine Client files to version 4.5.1, you must remove the version 4.0 Client files.

If you are performing a staged upgrade, and are upgrading Application Engine before you upgrade Content Engine, it is not necessary to do this task at this time. When you upgrade Content Engine to 4.5, you must then use this task to run the 4.5 Content Engine Client installer on your Application Engine, and redeploy the Workplace application.

Perform the following procedure to identify and uninstall all Content Engine Client version 4.0 files on an Application Engine Server machine. Repeat the procedure for all other Application Engine Server machines.

Depending on the CE Client fixpack versions that you have installed, you might have more than one instance of the CE Client 4.0 installed. Additionally, the version 4.0 CE Client installer supported installing multiple instance of the CE Client on the same server. You must uninstall all instances before upgrading to the 4.5 version of CE Client.

“Removing Content Engine 4.0 Client files from Application Engine servers (UNIX)”

The Content Engine 4.0 Client installation includes a UNIX tool for uninstalling the Client files.

“Removing Content Engine 4.0 Client files from Application Engine servers (Windows)”

The Content Engine 4.0 Client installation includes a Windows tool for uninstalling the Client files.

## Removing Content Engine 4.0 Client files from Application Engine servers (UNIX)

The Content Engine 4.0 Client installation includes a UNIX tool for uninstalling the Client files.

To uninstall Content Engine Client 4.0. instances:

1. Run one of the following commands, depending on the fixpack version of Content Engine Client that is installed:

```
/ce_client_install_path/ClientUpdater/_uninst/uninstaller.bin
```

```
/ce_client_install_path/CEClient/_CEClientuninst/uninstaller
```

Prior to fix pack P8CE-4.0.1-006 : The Content Engine Client files are in a directory called `ClientUpdater`, and the uninstallation program is `.../ClientUpdater/_uninst/uninstaller.bin..`

As of fix pack P8CE-4.0.1-006: The Content Engine Client files are in a directory called `CEClient` and the uninstallation program is `.../CEClient/_CEClientuninst/uninstaller`.

2. In the Uninstall IBM FileNet Client Installer screen, click **Next**.
3. In the Select Components screen, select Complete Uninstall. Click **Next**.
4. In the Uninstall Complete screen, click **Done**.
5. Repeat these steps for each additional instance of Content Engine Client updater or installer programs on this server.

## Removing Content Engine 4.0 Client files from Application Engine servers (Windows)

The Content Engine 4.0 Client installation includes a Windows tool for uninstalling the Client files.

To uninstall Content Engine Client 4.0 instances:

1. Select **Start** → **Settings** → **Control Panel** → **Add/Remove Programs**.
2. Select **Content Engine Client Updater** or **IBM FileNet Content Engine Client Installer**, depending on the fixpack version of Content Engine Client that is installed.

Prior to fix pack P8CE-4.0.1-006: The Content Engine Client is named Content Engine Client Updater.

As of fix pack P8CE-4.0.1-006: The Content Engine Client is named IBM FileNet Content Engine Client Installer.

3. Click **Change/Remove** to start the uninstaller.
4. In the Uninstall IBM FileNet Content Engine Client Installer screen, click **Next**.
5. In the Select Components screen, select Complete Uninstall. Click **Next**.
6. In the Uninstall Complete screen, click **Done**.
7. Repeat these steps for each additional instance of Content Engine Client updater or installer programs in the **Add/Remove Programs** list.

## Installing the latest Content Engine Client files on Application Engine servers interactively

The installation wizard provides an interactive way to install the Content Engine Client files. You can use the values you collected on your worksheet to fill in the required value for each field on the wizard screens.

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

To install the Content 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 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 (UNIX), on the machine where Application Engine is installed
  - Execute permission on the Content Engine Client install software
3. Verify that there is a current backup of the Application Engine.
4. Copy the Content Engine Client installation software from the Content Engine installation software to the temporary directory. The version of the client installation software must match the version of Content Engine.
5. Expand the compressed Content Engine Client installation software file in the temporary directory.
6. Close all instances of Workplace and any other Application Engine client applications. From the application server administrative console, stop and undeploy Application Engine.

Option	Description
WebSphere Application Server	Stop and undeploy the Application Engine Web application.
Oracle WebLogic Server	Stop and undeploy the Application Engine Web application.
JBoss Application Server	Run the shutdown command.

7. (WebLogic Server only) Manually delete the following application server cache directories and substitute your domain name in place of *mydomain*:

Option	Description
WebLogic Server on UNIX	<p>/opt/bea/user_projects/domains/<i>mydomain</i>/servers/AdminServer/tmp/_WL_user/app_engine</p> <p>/opt/ bea/user_projects/domains/<i>mydomain</i>/servers/.wlnotdelete</p> <p>/opt/bea/user_projects/domains/<i>mydomain</i>/servers/AdminServer/cache/EJBCompilerCache</p>

Option	Description
WebLogic Server on Windows	<p>C:\bea\user_projects\domains\mydomain\servers\AdminServer\tmp\_WL_user\app_engine</p> <p>C:\bea\user_projects\domains\mydomain\servers\.wlnotdelete</p> <p>C:\bea\user_projects\domains\mydomain\servers\AdminServer\cache\EJBCompilerCache</p>


8. Access the IBM FileNet Content Engine client update software in the temporary directory.
9. Start the installation program by running the following command, where *CE\_version* is the version of Content Engine you intend to run, for example, 4.5.1.

Operating System	Install Program
AIX	P8CE-CLIENT-CE_version-AIX.BIN
HPUX	P8CE-CLIENT-CE_version-HPUX.BIN
HPUXi	P8CE-CLIENT-CE_version-HPUXI.BIN
Linux	P8CE-CLIENT-CE_version-LINUX.BIN
Solaris	P8CE-CLIENT-CE_version-SOL.BIN
Windows	P8CE-CLIENT-CE_version-WIN.EXE
Linux on System z	P8CE-CLIENT-CE_version-ZLINUX.BIN

10. Complete the installation screens by using the values from your installation worksheet.
11. When the installation completes, check the Content 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 Engine Client files:

Operating System	Path to Log File
UNIX	/opt/IBM/FileNet/CEClient/ceclient_install_log_4_5_1.txt
Windows	C:\Program Files\IBM\FileNet\CEClient\ceclient_install_log_4_5_1.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 Content Engine Client files silently

The command line method provides a way to silently install the Content 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.

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 **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 (UNIX), on the machine where Application Engine is installed
  - Execute permission on the Content Engine Client install software
3. Verify that there is a current backup of the Application Engine.
4. Copy the Content Engine Client installation software from the Content Engine installation software to the temporary directory. The version of the client installation software must match the version of Content Engine.
5. Expand the compressed Content Engine Client installation software file in the temporary directory.
6. Close all instances of Workplace and any other Application Engine client applications. From the application server administrative console, stop and undeploy Application Engine.

Option	Description
WebSphere Application Server	Stop and undeploy the Application Engine Web application.
Oracle WebLogic Server	Stop and undeploy the Application Engine Web application.
JBoss Application Server	Run the shutdown command.

7. (WebLogic Server only) Manually delete the following application server cache directories and substitute your domain name in place of *mydomain*:

Option	Description
WebLogic Server on UNIX	<p>/opt/bea/user_projects/domains/<i>mydomain</i>/servers/AdminServer/tmp/_WL_user/app_engine</p> <p>/opt/ bea/user_projects/domains/<i>mydomain</i>/servers/.wlnotdelete</p> <p>/opt/bea/user_projects/domains/<i>mydomain</i>/servers/AdminServer/cache/EJBCompilerCache</p>
WebLogic Server on Windows	<p>C:\bea\user_projects\domains\<i>mydomain</i>\servers\AdminServer\tmp\_WL_user\app_engine</p> <p>C:\bea\user_projects\domains\<i>mydomain</i>\servers\wlnotdelete</p> <p>C:\bea\user_projects\domains\<i>mydomain</i>\servers\AdminServer\cache\EJBCompilerCache</p>

8. Make a backup copy of the CEClient\_silent\_install.txt input file in the temporary directory.
9. 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.


10. Navigate to the temporary directory path containing the Content Engine Client installation program.
11. Start the installation program by running the following command, where:
  - CE\_version* is the version of Content Engine you intend to run, for example, 4.5.1.
  - path* is the path that contains the installation program.

Operating System	Install Program
AIX	P8CE-CLIENT- <i>CE_version</i> -AIX.BIN -f <i>path</i> /CEClient.AIX/ CEClient_silent_install.txt -i silent
HPUX	P8CE-CLIENT- <i>CE_version</i> -HPUX.BIN -f <i>path</i> /CEClient.HPUX/ CEClient_silent_install.txt -i silent
HPUXi	P8CE-CLIENT- <i>CE_version</i> -HPUXI.BIN -f <i>path</i> /CEClient.HPUXI/ CEClient_silent_install.txt -i silent
Linux	P8CE-CLIENT- <i>CE_version</i> -LINUX.BIN -f <i>path</i> /CEClient.Linux/ CEClient_silent_install.txt -i silent
Solaris	P8CE-CLIENT- <i>CE_version</i> -SOL.BIN -f <i>path</i> /CEClient.Solaris/ CEClient_silent_install.txt -i silent
Windows	P8CE-CLIENT- <i>CE_version</i> -WIN.EXE -f <i>path</i> \CEClient.Windows\ CEClient_silent_install.txt -i silent
Linux on System z	P8CE-CLIENT- <i>CE_version</i> -ZLINUX.BIN -f <i>path</i> /CEClient.zLinux/ CEClient_silent_install.txt -i silent

12. When the installation completes, check the Content 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 Engine Client files:

Operating System	Path to Log File
UNIX	/opt/IBM/FileNet/CEClient/ ceclient_install_log_4_5_1.txt
Windows	C:\Program Files\IBM\FileNet\CEClient\ ceclient_install_log_4_5_1.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 Process Engine client files on Application Engine servers

The Process Engine Client software enables communication between the Application Engine and the Process Engine. You must install the Process Engine Client files on all Application Engine servers.



“Upgrading the latest Process Engine Client files interactively”

The installation wizard provides an interactive way to upgrade the Process Engine Client files. You can use the values you collected on your worksheet to fill in the required value for each field on the wizard screens.

“Upgrading the latest Process Engine Client files silently” on page 456

You can upgrade the Process Engine Client software on the Application Engine by using a silent input text file and running the installation program from the command line. Use the values in your upgrade worksheet to edit the silent input text file before you run the upgrade.

## Upgrading the latest Process Engine Client files interactively

The installation wizard provides an interactive way to upgrade the Process Engine Client files. You can use the values you collected on your worksheet to fill in the required value for each field on the wizard screens.

To upgrade the Process Engine Client 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 Process Engine values, filter by **PE Client Installer** in the **Installation or Configuration Program** column.

2. On the machine where Application Engine is to be deployed, log on as any user who has the following permissions:
  - Read and write permission to a temporary directory, such as temp (Windows) or tmp (UNIX), on the machine where Application Engine is installed.
  - Execute permission on the Process Engine Client install software.
3. Copy the Process Engine Client install software from the Process Engine installation software to the temporary directory. The version of the install software must match the version of Process Engine.
4. Expand the compressed Process Engine Client install software file within the temporary directory. The jre.tar file that is packaged with the Process Engine Client installer must be in the same directory as the Process Engine Client installer when the installer is run.
5. The expanded install software contains the Process Engine Client install program specific to the operating system on the machine where Application Engine is deployed.

To run the program interactively, run one of the commands in the table below, and complete the screens.

Operating System	Install Program
AIX	P8PE-CLIENT-PE_version-AIX.BIN
HPUX	P8PE-CLIENT-PE_version-HPUX.BIN
HPUXi	P8PE-CLIENT-PE_version-HPUXI.BIN
Linux	P8PE-CLIENT-PE_version-LINUX.BIN
Solaris	P8PE-CLIENT-PE_version-SOL.BIN
Windows	P8PE-CLIENT-PE_version-WIN.EXE
Linux on System z	P8PE-CLIENT-PE_version-ZLINUX.BIN


6. For Process Engine upgrades from version 4.0 only, add required JAR files to the Component Manager library. Launch the Process Task Manager by running

one of the following command files from the AE\_install\_path/FileNet/AE/Router directory, depending on your operating system:

Option	Description
UNIX	routercmd.sh
Windows	routercmd.bat

- a. In the Process Task Manager console, under Application Engine, **Component Manager** node, before starting up any existing router, click the **Required** libraries tab.
- b. Click **Add** and browse to /Router/lib.
- c. Select the following files to add:
  - ContentExtended0ps.jar
  - smtp.jar
  - pe3pt.jar

#### 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*.

## Upgrading the latest Process Engine Client files silently

You can upgrade the Process Engine Client software on the Application Engine by using a silent input text file and running the installation program from the command line. Use the values in your upgrade worksheet to edit the silent input text file before you run the upgrade.

To upgrade the Process Engine Client 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 Process Engine values, filter by **PE Client Installer** in the **Installation or Configuration Program** column.

2. On the machine where Application Engine is to be deployed, log on as any user who has the following permissions:
  - Read and write permission to a temporary directory, such as temp (Windows) or tmp (UNIX), on the machine where Application Engine is installed.
  - Execute permission on the Process Engine Client install software.
3. Copy the Process Engine Client install software from the Process Engine installation software to the temporary directory. The version of the install software must match the version of Process Engine.
4. Expand the compressed Process Engine Client install software file within the temporary directory. The jre.tar file that is packaged with the Process Engine Client installer must be in the same directory as the Process Engine Client installer when the installer is run.
5. The expanded install software contains the Process Engine Client install program specific to the operating system on the machine where Application Engine is deployed.
6. In the expanded install software, open the file PEClient\_silent\_install.txt and change the Variable\_CheckboxAE line to the following value:  
-V Variable\_CheckboxAE="true"

7. Choose one of the following commands to run the silent installation:


Operating System	Install Program
AIX	P8PE-CLIENT- <i>PE_version</i> -AIX.BIN -silent -options "PEClient_silent_install.txt"
HPUX	P8PE-CLIENT- <i>PE_version</i> -HPUX.BIN -silent -options "PEClient_silent_install.txt"
HPUXi	P8PE-CLIENT- <i>PE_version</i> -HPUXI.BIN -silent -options "PEClient_silent_install.txt"
Linux	P8PE-CLIENT- <i>PE_version</i> -LINUX.BIN -silent -options "PEClient_silent_install.txt"
Solaris	P8PE-CLIENT- <i>PE_version</i> -SOL.BIN -silent -options "PEClient_silent_install.txt"
Windows	P8PE-CLIENT- <i>PE_version</i> -WIN.EXE -silent -options "PEClient_silent_install.txt"
Linux on System z	P8PE-CLIENT- <i>PE_version</i> -ZLINUX.BIN -silent -options "PEClient_silent_install.txt"

8. For Process Engine upgrades from version 4.0 only, add required JAR files to the Component Manager library. Launch the Process Task Manager by running one of the following command files from the AE\_install\_path/FileNet/AE/Router directory, depending on your operating system:

Option	Description
UNIX	routercmd.sh
Windows	routercmd.bat

- a. In the Process Task Manager console, under Application Engine, **Component Manager** node, before starting up any existing router, click the **Required** libraries tab.
- b. Click **Add** and browse to /Router/lib.
- c. Select the following files to add:
  - ContentExtendedOps.jar
  - smtp.jar
  - pe3pt.jar

#### 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 upgrades from 3.5

After you complete the Application Engine upgrade from 3.5, you must configure Application Engine files and your application sever to enable communication between Application Engine and Content Engine. You can choose the appropriate configuration tasks for your application server type and environment.

“Configuring Application Engine upgrades from 3.5 on WebSphere Application Server” on page 458

After you upgrade the Application Engine server from 3.5, you must configure WebSphere Application Server to work with Application Engine. You can also configure changes for optional modes like SSO.

“Configuring Application Engine upgrades from 3.5 on WebLogic Server” on page 470

After you upgrade the Application Engine server from version 3.5, you must configure WebLogic Server to work with Application Engine. You can also configure changes for optional modes like SSO.

“Configuring Application Engine upgrades from 3.5 on JBoss Application Server” on page 475

After you upgrade the Application Engine server from version 3.5, you must configure JBoss Application Server to work with Application Engine. You can also configure changes for optional modes like SSO.

## Configuring Application Engine upgrades from 3.5 on WebSphere Application Server

After you upgrade the Application Engine server from 3.5, you must configure WebSphere Application Server to work with Application Engine. You can also configure changes for optional modes like SSO.

“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.

“Editing web.xml for SSO” on page 461

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 465

You can 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 466

To set up LTPA security, configure settings to match on both the Content Engine application server and the Application Engine application server. If your Application Engine and Content Engine are on the same WebSphere Application Server, it is not necessary to configure LTPA.

“Configuring stand-alone Lightweight Directory Access Protocol (LDAP)” on page 468

To enable LDAP communication between Application Engine and Content Engine, you must configure settings on the WebSphere Application Server.

“Configuring Lightweight Directory Access Protocol (LDAP) for federated repositories” on page 469

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.

### 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 below.

```
<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>/portlets/Author/edit.jsp</url-pattern>
<url-pattern>/portlets/Author/portlet.jsp</url-pattern>
<url-pattern>/portlets/Browse/edit.jsp</url-pattern>
<url-pattern>/portlets/Browse/portlet.jsp</url-pattern>
<url-pattern>/portlets/ExternalUrl/edit.jsp</url-pattern>
<url-pattern>/portlets/ExternalUrl/portlet.jsp</url-pattern>
<url-pattern>/portlets/GroupPageDesign.jsp</url-pattern>
<url-pattern>/portlets/GroupPageSettings.jsp</url-pattern>
<url-pattern>/portlets/Inbox/edit.jsp</url-pattern>
<url-pattern>/portlets/Inbox/portlet.jsp</url-pattern>
<url-pattern>/portlets/MultiPagesDesign.jsp</url-pattern>
<url-pattern>/portlets/OrganizePages.jsp</url-pattern>
<url-pattern>/portlets/PortalPageDesign.jsp</url-pattern>
<url-pattern>/portlets/PortalPageInfo.jsp</url-pattern>
<url-pattern>/portlets/PortletAlias.jsp</url-pattern>
<url-pattern>/portlets/PortletSettings.jsp</url-pattern>
<url-pattern>/portlets/PreviewAndSetup.jsp</url-pattern>
<url-pattern>/portlets/PublicQueue/edit.jsp</url-pattern>
<url-pattern>/portlets/PublicQueue/portlet.jsp</url-pattern>
<url-pattern>/portlets/QuickSearch/edit.jsp</url-pattern>
<url-pattern>/portlets/QuickSearch/portlet.jsp</url-pattern>
<url-pattern>/portlets/Workflows/edit.jsp</url-pattern>
<url-pattern>/portlets/Workflows/portlet.jsp</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>/WcmPortletHelp.jsp</url-pattern>
<url-pattern>/WcmPortletSearch.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>/vwsimsoapservlet</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 wild-card (\*) `<role-name>` as noted in the file comments below.

```

<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 section `<auth-constraint>`, comment the wild-card (\*) `<role-name>` as noted in the file comments below.

```

<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>

```

6. 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>

```

7. 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>

```

8. 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 below.

```

<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>/portlets/Author/edit.jsp</url-pattern>
<url-pattern>/portlets/Author/portlet.jsp</url-pattern>
<url-pattern>/portlets/Browse/edit.jsp</url-pattern>
<url-pattern>/portlets/Browse/portlet.jsp</url-pattern>
<url-pattern>/portlets/ExternalUrl/edit.jsp</url-pattern>
<url-pattern>/portlets/ExternalUrl/portlet.jsp</url-pattern>
<url-pattern>/portlets/GroupPageDesign.jsp</url-pattern>
<url-pattern>/portlets/GroupPageSettings.jsp</url-pattern>
<url-pattern>/portlets/Inbox/edit.jsp</url-pattern>
<url-pattern>/portlets/Inbox/portlet.jsp</url-pattern>
<url-pattern>/portlets/MultiPagesDesign.jsp</url-pattern>
<url-pattern>/portlets/OrganizePages.jsp</url-pattern>
<url-pattern>/portlets/PortalPageDesign.jsp</url-pattern>
<url-pattern>/portlets/PortalPageInfo.jsp</url-pattern>
<url-pattern>/portlets/PortletAlias.jsp</url-pattern>
<url-pattern>/portlets/PortletSettings.jsp</url-pattern>
<url-pattern>/portlets/PreviewAndSetup.jsp</url-pattern>
<url-pattern>/portlets/PublicQueue/edit.jsp</url-pattern>
<url-pattern>/portlets/PublicQueue/portlet.jsp</url-pattern>
<url-pattern>/portlets/QuickSearch/edit.jsp</url-pattern>
<url-pattern>/portlets/QuickSearch/portlet.jsp</url-pattern>
<url-pattern>/portlets/Workflows/edit.jsp</url-pattern>
<url-pattern>/portlets/Workflows/portlet.jsp</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>/WcmPortletHelp.jsp</url-pattern>
<url-pattern>/WcmPortletSearch.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>/vwsimsoapservlet</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 wild-card (\*) `<role-name>` as noted in the file comments below.

```

<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>

```

- At the end of `web.xml`, comment out the `<login-config>` element, as follows:

```

<!--
<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>
-->

```

- 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.

The default settings are (in **bold** below):

```

<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 parameters above 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 values:

```

<param-name>ssoProxyContextPath</param-name>
<param-value>/Workplace</param-value>

```

#### **ssoProxyHost**

Set the value to the SSO proxy host server name. Typically, this will be a full domain-qualified hostname.

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 values:

```
<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 and/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**

You can 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.

1. Log in to the WebSphere administrative console.
2. Navigate to the Java Virtual Machine settings.

Option	Description
WebSphere Application Server 6.1	Servers → Application Servers → <i>server_name</i> → Java & Process Management → Process Definition → Java Virtual Machine
WebSphere Application Server 7.0	Servers → Server Types → WebSphere application servers → <i>server_name</i> > 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, such as:

**UNIX** /opt/FileNet/AE

#### **Windows**

C:\Progra~1\FileNet\AE

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.

**Important:** (Windows only) The path cannot contain a space. You must use 8.3-notation for the install path portion of the full JAAS login entry described above.

If `AE_install_path` is: `C:\Program Files\FileNet\AE`

use: `C:\Progra~1\FileNet\AE`

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 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 Engine profile and the Application Engine profile:

- a. In the Java Virtual Machine settings, create a new 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 Performance Tuning Guide, as well as PDF's of the rest of 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 Engine application server and the Application Engine application server. If your Application Engine and Content Engine are on the same WebSphere Application Server, it is not necessary to configure LTPA.

If you are already using LTPA with your Content Engine application server, export the existing keys and copy the key file to the Application Engine server. Check with your Content Engine administrator.

To configure LTPA, take the following steps:

1. On the Content Engine server, log in to the WebSphere administrative console.
2. Navigate to the LTPA settings page.

Option	Description
WebSphere Application Server 6.1	<ol style="list-style-type: none"> <li>1. Navigate to <b>Security &gt; Secure administration, applications, and infrastructure</b>.</li> <li>2. From the right side of the panel, select <b>Authentication Mechanisms and expiration</b>.</li> </ol>
WebSphere Application Server 7.0	<ol style="list-style-type: none"> <li>1. Navigate to <b>Security &gt; Global security</b>.</li> <li>2. From the right side of the panel, select <b>LTPA</b>.</li> </ol>

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.
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 Engine for LTPA, use the existing password in the Application Engine configuration below.
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 similar to 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 WebSphere Application Server.
10. Copy the key file from the Content Engine server location you specified above 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.

Option	Description
WebSphere Application Server 6.1	<ol style="list-style-type: none"> <li>1. Navigate to <b>Security &gt; Secure administration, applications, and infrastructure</b>.</li> <li>2. From the right side of the panel, select <b>Authentication Mechanisms and expiration</b>.</li> </ol>
WebSphere Application Server 7.0	<ol style="list-style-type: none"> <li>1. Navigate to <b>Security &gt; Global security</b>.</li> <li>2. From the right side of the panel, select <b>LTPA</b>.</li> </ol>

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.
14. Save your changes.

15. In the box for **Cross-cell single sign-on**, type and confirm the **LTPA password** you created for Content Engine.  
For password restrictions, see the WebSphere Application Server documentation. If you have already configured Content Engine for LTPA, use the existing password in the Application Engine configuration below.
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 similar to the following one is displayed: The keys were successfully imported from the file `ltpa_key_name`.
18. Save your changes.

## 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.

To configure stand-alone Lightweight Directory Access Protocol (LDAP):

1. Open the WebSphere administrative console.
2. Navigate to **Security > Secure administration, applications, and infrastructure**.
3. Disable security using the following Security settings:
  - Clear the **Enable Administrative Security** flag.
  - Clear the **Enable application security** flag.
  - 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. Re-enable the following Security settings:
    - Select the **Enable Administrative Security** flag.
    - Select the **Enable application security** flag.
    - 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. 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.

**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.

To configure Lightweight Directory Access Protocol (LDAP) for federated repositories:

1. Open the WebSphere administrative console.
2. Navigate to the security settings page.

Option	Description
WebSphere Application Server 6.1	Navigate to <b>Security &gt; Secure administration, applications, and infrastructure</b> .
WebSphere Application Server 7.0	Navigate to <b>Security &gt; Global security</b> .

3. Disable the following Security settings:
  - Clear the **Enable Administrative Security** flag.
  - Clear the **Enable application security** flag.
  - 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. Re-enable the following Security settings:
    - Select the **Enable Administrative Security** flag.
    - Select the **Enable application security** flag.
    - 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.
  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.

## Configuring Application Engine upgrades from 3.5 on WebLogic Server

After you upgrade the Application Engine server from version 3.5, you must configure WebLogic Server to work with Application Engine. You can also configure changes for optional modes like SSO.

*“Editing web.xml for SSO (optional)”*

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 WebLogic Server.

*“Configuring the application server files” on page 472*

As part of the configuration of Application Engine on WebLogic Server, configure the application server files to set up JAAS login information for authentication and memory settings for resource usage.

*“Enabling communication between Content Engine and Application Engine (WebLogic Server)” on page 474*

To enable communication between Application Engine and Content Engine, you must configure settings on the WebLogic Server.

*“Enabling passing user credentials to client applications (WebLogic Server 9.2 only)” on page 475*

Some client applications such as WebDAV and Application Integration can require passing user credentials with Application Engine. Enable this communication by editing the config.xml file on the WebLogic Server.

### Editing web.xml for SSO (optional)

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 WebLogic Server.

To edit web.xml for SSO

1. Make a backup copy of web.xml.  
`AE_install_path/Workplace/WEB-INF/web.xml`

2. Open web.xml for editing.
3. Set the parameter `perimeterChallengeMode` to true:

```
<init-param>
<param-name>perimeterChallengeMode</param-name>
<param-value>true</param-value>
</init-param>
```

4. 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, then you must set the corresponding `sso*` 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 parameters above should 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 values:

```
<param-name>ssoProxyContextPath</param-name>
<param-value>/fn/Workplace</param-value>
```

#### **ssoProxyHost**

Set the value to the SSO proxy host server name. Typically, this will be a full domain-qualified hostname.

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 values:

```
<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 and/or used to access Workplace pages.

For example:

```
<param-name>ssoProxySSLPort</param-name>
<param-value>443</param-value>
```

5. Save your changes to `web.xml` and close the file.

## Configuring the application server files

As part of the configuration of Application Engine on WebLogic Server, configure the application server files to set up JAAS login information for authentication and memory settings for resource usage.

To modify the application server files:

1. Stop the WebLogic Server if it is running.
2. Make a backup copy of the `setDomainEnv` file.

For Windows, back up `setDomainEnv.cmd`.

For UNIX, back up `setDomainEnv.sh`.

3. Edit the `MEM_ARGS` variable.

Adjusting this setting prevents the application server from running out of memory, a condition in which users would not be able to log in to Workplace.

If the `MEM_ARGS` variable does not exist, add it to the startup script.

- For all systems except those using JRockit JAVA.

Append the following to the `MEM_ARGS` variable:

```
-XX:MaxPermSize= size m
```

where *size* is the value, in MB, of the **MaxPermSize**.

Refer to your application server vendor recommendation for Initial and Maximum heap size values. For IBM specific recommendations, see the *IBM FileNet P8 Performance Tuning Guide*.

- For systems using JRockit JAVA.

Append the following to the `MEM_ARGS` variable:

```
-Xgc:gencon
```

4. If your application server uses the IBM JVM, edit the `JAVA_OPTIONS` variable to improve performance.

### UNIX

Immediately before the following line in the `setDomainEnv` file:

```
SAVE_JAVA_OPTIONS=$JAVA_OPTIONS
```

insert this line (without a carriage return):

```
JAVA_OPTIONS="$JAVA_OPTIONS -Dprogram.name=$PROGNAME
-DfileNet.pe.peorb.pool.min=2 -DfileNet.pe.peorb.pool.max=5"
```

### Windows

Immediately before the following line in the `setDomainEnv` file

```
set SAVE_JAVA_OPTIONS=%JAVA_OPTIONS%
```

insert this line (no carriage return):

```
set JAVA_OPTIONS=%JAVA_OPTIONS% -Dprogram.name=%PROGNAME%
-DfileNet.pe.peorb.pool.min=2 -DfileNet.pe.peorb.pool.max=5
```

5. Configure JAAS login.

Add one of the following right after the classpath entry for WebLogic Server.

**Important:** Enter the `jaas_login` entry as a single line without line breaks. Do not copy and paste the text from this guide because hidden formatting can cause problems with the entry. Instead, type the entry into the script.

**Tip:** Your path might be slightly different depending on the version of your client installations, or whether you have chosen a custom path for installation. Verify the location of the file before you enter the path.

**UNIX**

```
Jaas Login configuration setting
JAAS_LOGIN="{JAAS_LOGIN}" -Djava.security.auth.login.config=
"AE_install_path/CE_API/config/jaas.conf.WebLogic"
```

**AIX**

```
Jaas Login configuration setting
JAAS_LOGIN="{JAAS_LOGIN}" -Djava.security.auth.login.config=
"AE_install_path/CE_API/config/jaas.conf.WebLogic"
JAAS_LOGIN="{JAAS_LOGIN}"
-Dlogin.configuration.provider=com.ibm.security.auth.login.ConfigFile
```

**Windows**

```
@REM Jaas Login configuration setting
set JAAS_LOGIN=%JAAS_LOGIN% -Djava.security.auth.login.config=
"AE_install_path\CE_API\config\jaas.conf.WebLogic"
```

6. Make a backup copy of the application server startup script.

For Windows, back up `startWebLogic.cmd`.

For UNIX, back up `startWebLogic.sh`

If you are not using a WebLogic domain, back up these files:

For Windows, back up `startWLS.cmd`

For UNIX, back up `startWLS.sh`.

7. Add the `%JAAS_LOGIN%` section to the application server startup script as indicated in the following examples.

**UNIX - in the WLS\_REDIRECT\_LOG settings**

```
{JAVA_HOME}/bin/java {JAVA_VM} -version


if ["${WLS_REDIRECT_LOG}" = ""] ; then
echo "Starting WLS with line:"
echo "{JAVA_HOME}/bin/java {JAVA_VM} {MEM_ARGS} {JAVA_OPTIONS}
-Dweblogic.Name={SERVER_
NAME} -Djava.security.policy={WL_HOME}/server/lib/weblogic.policy
{PROXY_SETTINGS} {SERVER_CLASS}
}"
{JAVA_HOME}/bin/java {JAVA_VM} {MEM_ARGS} {JAVA_OPTIONS}
{JAAS_LOGIN} -Dweblogic.Name={SERVER_NAME}
-Djava.security.policy={WL_HOME}/server/lib/weblogic.policy
{PROXY_SETTINGS} {SERVER_
CLASS}
else
echo "Redirecting output from WLS window to {WLS_REDIRECT_LOG}"
{JAVA_HOME}/bin/java {JAVA_VM} {MEM_ARGS} {JAVA_OPTIONS}
{JAAS_LOGIN} -Dweblogic.Name={SERVER_NAME}
-Djava.security.policy={WL_HOME}/server/lib/weblogic.policy
{PROXY_SETTINGS} {SERVER_
CLASS} >"{WLS_REDIRECT_LOG}" 2>&1
fi
```

## Windows - in the WLS\_REDIRECT\_LOG settings

```
If "%WLS_REDIRECT_LOG%"==" "(
echo Starting WLS with line:
echo %JAVA_HOME%\bin\java %JAVA_VM% %MEM_ARGS% %JAVA_OPTIONS%
%JAAS_LOGIN% -Dweblogic.Name=%SERVER_NAME%
-Djava.security.policy=%WL_HOME%\server\lib\weblogic.policy
%PROXY_SETTINGS% %SERVER_CLASS% %JAVA_HOME%\bin\java %JAVA_VM%
%MEM_ARGS% %JAVA_OPTIONS% %JAAS_LOGIN%
-Dweblogic.Name=%SERVER_NAME%
-Dweblogic.management.username=%WLS_USER%
-Dweblogic.management.password=%WLS_PW%
-Djava.security.policy=%WL_HOME%\server\lib\weblogic.policy
%PROXY_SETTINGS% %SERVER_CLASS%
) else (
echo Redirecting output from WLS window to %WLS_REDIRECT_LOG%
%JAVA_HOME%\bin\java %JAVA_VM% %MEM_ARGS% %JAVA_OPTIONS%
%JAAS_LOGIN% -Dweblogic.Name=%SERVER_NAME%
-Dweblogic.management.username=%WLS_USER%
-Dweblogic.management.password=%WLS_PW%
-Djava.security.policy=%WL_HOME%\server\lib\weblogic.policy
%PROXY_SETTINGS% %SERVER_CLASS% >"%WLS_REDIRECT_LOG%" 2>&1
)
```

8. Save and close the application server startup script.

### Related information

 [Product documentation for IBM FileNet P8 Platform](#)

Download the IBM FileNet P8 Performance Tuning Guide, as well as PDF's of the rest of the IBM FileNet P8 Platform documentation.

## Enabling communication between Content Engine and Application Engine (WebLogic Server)

To enable communication between Application Engine and Content Engine, you must configure settings on the WebLogic Server.

To configure Application Engine:

1. (If you selected Container-Managed Authentication during the installation)  
Enable trust between WebLogic domains for the Content Engine domain and the Application Engine domain.  
Do the following on both the Content Engine application server and the Application Engine application server.
  - a. In the WebLogic Administration Console, in the security settings, enter a password for the domain. You must enter the same password for both the Content Engine domain and Application Engine domain.
  - b. Save your changes.
  - c. Restart the server if needed.
  - d. Repeat this procedure in each domain for which you want to enable trust.
2. (If you selected Container-Managed Authentication during the installation)  
Configure LDAP settings on Application Engine to exactly match the Content Engine settings.
  - a. See your Content Engine installation worksheet items and the Administration Console settings for Compatibility Security > Realms for Authentication Provider, users, and groups on Content Engine.  
Configure the LDAP provider to exactly match the settings from the Content Engine server:
    - Group Base DN
    - User Name Attribute

- Port
  - User Base DN
  - Principal
  - Credential
  - Confirm Credential
  - Host
  - User From Name Filter
  - Group From Name Filter
- b. Restart WebLogic.
3. Set permissions for the user running the application server.  
If the user that will be running the application server is different from the user that installed Application Engine, you must give the user read/write permissions on the folder where you installed Application Engine (*AE\_install\_path*).

### Enabling passing user credentials to client applications (WebLogic Server 9.2 only)

Some client applications such as WebDAV and Application Integration can require passing user credentials with Application Engine. Enable this communication by editing the `config.xml` file on the WebLogic Server.

**Important:** If you do not make this change to `config.xml`, then end users will be prompted to enter their user name and password to complete any client operations, such as adding a document.

To enable passing user credentials:

1. Stop the WebLogic server.
2. Make a backup copy of `config.xml` located in deployment directory.  
For example: `BEA_home/bea/user_projects/domains/domain_name/config/config.xml`
3. Edit `config.xml`.

**Important:** The `enforce-valid-basic-auth-credentials` entry should be entered as a single line without line breaks.

- a. Locate the `<security-configuration>` section and add the following line to the end of the section, just before the `</security-configuration>` tag:
 

```
<enforce-valid-basic-auth-credentials>>false
</enforce-valid-basic-auth-credentials>
```
  - b. Save your changes to `config.xml` and close the file.
4. Restart WebLogic.

## Configuring Application Engine upgrades from 3.5 on JBoss Application Server

After you upgrade the Application Engine server from version 3.5, you must configure JBoss Application Server to work with Application Engine. You can also configure changes for optional modes like SSO.

To configure JBoss Application Server for Application Engine:

1. Stop JBoss Application Server if it is running.



2. Make a backup copy of the run.conf file and the startup script, depending on your platform:

Option	Description
UNIX	run.sh
Windows	run.bat

3. Edit the run.conf file Java settings.
  - a. Add a line to specify the path to the JDK provided by JBoss Application Server, as shown in the following example (Windows): set  
 JAVA\_HOME=C:\Program Files\Java\jdk1.5.0\_06  
  
**Important:** If your JDK is different from version 1.5.0, substitute your version for the one listed above.
  - b. Update the JAVA\_OPTS memory settings.  
 Adjusting this setting prevents the application server from running out of memory, a condition in which users would not be able to log in to Workplace.  
 In the JAVA\_OPTS line, change the -Xms and -Xmx values (**bold**) for your configuration.  
 Example (Windows): set JAVA\_OPTS=%JAVA\_OPTS% -Xms 128m -Xmx 512 m  
 See your application server vendor's recommendation for Initial and Maximum heap size values. For IBM specific recommendations, see the *IBM FileNet P8 Performance Tuning Guide*.
  - c. (Sun JVM users only) Set the value of MaxPermSize in JAVA\_OPTS to 128m, as follows:  
 UNIX  
 JAVA\_OPTS=%JAVA\_OPTS% -Xms128m -Xmx512m -XX:MaxPermSize=128m  
 Windows  
 set JAVA\_OPTS=%JAVA\_OPTS% -Xms128m -Xmx512m -XX:MaxPermSize=128m  
 This increased value prevents out of memory errors that can stop JBoss Application Server.
  - d. If your application server uses the IBM JVM, edit the JAVA\_OPTS variable in the run.conf file immediately after the line in the previous sub-step. This JAVA\_OPTS edit improves performance.  
**UNIX** Find the following line in the run.conf file:  
 JAVA\_OPTS="\$JAVA\_OPTS  
 and change it to this (without a carriage return):  
 JAVA\_OPTS="\$JAVA\_OPTS -Dfilenet.pe.peorb.pool.min=2  
 -Dfilenet.pe.peorb.pool.max=5"  
  
**Windows**  
 Find the following line in the run.conf file:  
 set JAVA\_OPTS=%JAVA\_OPTS%  
 and change it to this (without a carriage return):  
 set JAVA\_OPTS=%JAVA\_OPTS% -Dfilenet.pe.peorb.pool.min=2  
 -Dfilenet.pe.peorb.pool.max=5
  - e. Save your edits.
4. Configure JAAS login.

Add one of the following right after the "\$JAVA" \$JAVA\_OPTS (UNIX) or "%JAVA%" %JAVA\_OPTS (Windows) entry in the run.sh file for UNIX or the run.bat for Windows.

**Important:** Enter the jaas\_login entry (bold below) as a single line without line breaks. Do not copy and paste the text from this guide because hidden formatting can cause problems with the entry. Instead, type the entry into the script.

**Tip:** Your path might be slightly different depending on the version of your client installations, or whether you have chosen a custom path for installation. Verify the location of the file before you enter the path.

#### UNIX

```
"$JAVA" $JAVA_OPTS
-Djava.security.auth.login.config=
"/opt/FileNet/AE/CE_API/config/jaas.conf.JBoss"
-Djava.endorsed.dirs=$JBOSS_ENDORSED_DIRS" -classpath
"$JBOSS_CLASSPATH" org.jboss.Main $@
```

#### Windows

```
"%JAVA%" %JAVA_OPTS%
-Djava.security.auth.login.config=C:\Program
Files\FileNet\AE\CE_API\config\jaas.conf.JBoss"
-Djava.endorsed.dirs=%JBOSS_ENDORSED_DIRS%" -classpath
"%JBOSS_CLASSPATH%" org.jboss.Main %*
```

5. Save and close the run.sh file or the run.bat file.
6. Configure LDAP settings on Application Engine to exactly match the Content Engine settings.
  - a. On the Application Engine server, open login-config.xml , located in *JBoss\_home/server/server\_name/conf*, for editing.
  - b. Set the <application-policy name="FileNet"> entry identical to the corresponding entry in the login-config.xml file on the Content Engine server.
  - c. Set the <application-policy name="FileNetP8Engine"> entry identical to the corresponding entry in the login-config.xml file on the Content Engine server.
  - d. Copy the new <application-policy name="FileNetP8Engine"> entry, and paste the copied entry directly above entry you copied (<application-policy name="FileNetP8Engine">).
  - e. Change the first instance of the <application-policy name="FileNetP8Engine"> to <application-policy name="FileNetP8">.
  - f. Save changes to the login-config.xml file on the Application Engine server.
  - g. Restart JBoss Application Server.
7. Set permissions for the user running the application server.

On Windows, the following is only required for NTFS formatted partitions. If the user that will be running the application server is different from the user that installed Application Engine, you must give the user read and write permissions on the folder where you installed Application Engine (*AE\_install\_path*).
8. (Optional) Disable JBoss Application Server logging.

In development mode, JBoss Application Server creates a large number of HTTP Access, "INFO", "DEBUG" and "TRACE" log messages. This can cause

unexpected behavior in the deployed IBM FileNet software. Using the following procedure, you can limit this type of excessive JBoss Application Server logging.

When logging is disabled, error messages will still be displayed in the JBoss Application Server console.

- a. Open the `log4j.xml` file (*JBOSS\_home/server/server\_name/conf/log4j.xml*) for editing.
- b. Change all threshold values and priority values from "INFO", "DEBUG", or "TRACE" to "ERROR".
- c. Delete or comment out the "Preserve messages in a local file" to turn off the server log.
- d. To turn off HTTP access logging, open `jboss-service.xml` with a text editor and delete or comment out the "Access logger" section.

Location of `jboss-service.xml`:

*JBoss\_Home/server/server\_name/deploy/jbossweb-tomcat55.sar/META-INF*

- e. Open `web.xml` for editing and change the `logVerbosityLevel` to "FATAL".

Location of `web.xml`:

*JBoss\_Home/server/server\_name/deploy/jbossweb-tomcat55.sar/conf*

- f. Restart the JBoss Application Server server.

---

## Manually copying custom data

If your custom data was not retained in the upgrade, you must manually copy the data from the version 3.5 or 4.0.1 backup files (`deploy_backup`) to the upgraded directories.

You must also copy any data you want to retain if you have made any custom add-ons or modifications to the Application Engine installation being upgraded and chose not to keep these changes after the upgrade. You should manually copy any other custom data you want to retain to the upgraded files listed in "Preparing for Application Engine upgrade."

When you have completed the manual copy of your custom data, deploy the Workplace application.

### Related tasks

"Preparing for Application Engine upgrade" on page 440

Before you upgrade your Application Engine installation, you must prepare your existing configuration for the upgrade. This preparation includes backing up existing files and undeploying your web application.

---

## Deploying upgraded instances of Application Engine

After you upgrade and configure Application Engine, deploy your client application, Workplace, on your application server. It might be necessary to re-create the WAR or WAR and EAR files before you deploy.

"Deploying upgraded instances of Application Engine on WebSphere Application Server" on page 479

After you upgrade and configure Application Engine, deploy your client application, Workplace, on your WebSphere Application Server. It might be necessary to re-create the WAR or WAR and EAR files before you deploy.

"Deploying Application Engine on WebLogic Server" on page 482

After you install and configure Application Engine, you must deploy your

client application, Workplace, on your WebLogic Server. It might be necessary to re-create the WAR or WAR and EAR files before you deploy.

“Deploying Application Engine on JBoss Application Server” on page 484  
After you install and configure Application Engine, you must deploy your client application, Workplace, on your JBoss Application Server. It might be necessary to re-create the WAR or WAR and EAR files before you deploy.

## Deploying upgraded instances of Application Engine on WebSphere Application Server

After you upgrade and configure Application Engine, deploy your client application, Workplace, on your WebSphere Application Server. It might be necessary to re-create the WAR or WAR and EAR files before you deploy.

“Re-creating the WAR or EAR file”

Any time that you make changes to 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 Application Engine” on page 480

The method for deploying Application Engine varies depending on your WebSphere Application Server version.

### Re-creating the WAR or EAR file

Any time that you make changes to 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. Recreate the app\_engine.war file by running the script for your platform.

Option	Description
UNIX	<i>AE_install_path</i> /deploy/ create_app_engine_war.sh
Windows	<i>AE_install_path</i> \deploy\ create_app_engine_war.bat

3. (For WAR file deployment) Rename the newly recreated 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 will generate the following context root: `http://server_name:port# /app_engine`. Renaming the WAR file Workplace.war will generate 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 will by default create a file with the name app\_engine.war.

**Important:** Do not rename the WAR file if you are using the WAR file to recreate 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
UNIX	<code>AE_install_path/ deploy/ create_app_engine_ear.sh</code>
Windows	<code>AE_install_path\ deploy\ create_app_engine_ear.bat</code>

## Deploying Application Engine

The method for deploying Application Engine varies depending on your WebSphere Application Server version.

“Deploying the application (WebSphere Application Server 6.1)”

To use Workplace as a web application, you must deploy it as an application in the WebSphere 6.1 administrative console. You can specify the context root for the application URL during the deployment.

“Deploying the application (WebSphere Application Server 7.0)” on page 481

To use Workplace as a web application, you must deploy it as an application in the WebSphere 7.0 administrative console. You can specify the context root for the application URL during the deployment.

### Deploying the application (WebSphere Application Server 6.1):

To use Workplace as a web application, you must deploy it as an application in the WebSphere 6.1 administrative console. You can specify the context root for the application URL during the deployment.

To deploy Application Engine:

1. Log on to the WebSphere administrative console.
2. Navigate to **Applications > 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 pathname 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 in 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 application class loader first**.
10. Click **Apply**.
11. Click **Workplace > Manage Modules**.
12. Click **Workplace**.
13. Change the **Class loader order** to **Classes loaded with application class loader first**.

**Important:** Do this 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**. Verify that the **All Authenticated** column is checked for the "All Authenticated" role.
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.

### Deploying the application (WebSphere Application Server 7.0):

To use Workplace as a web application, you must deploy it as an application in the WebSphere 7.0 administrative console. You can specify the context root for the application URL during the deployment.

To deploy Application Engine:

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 pathname 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 in to by 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 dialog boxes for installing a new application by 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:** Do this 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.

## Deploying Application Engine on WebLogic Server

After you install and configure Application Engine, you must deploy your client application, Workplace, on your WebLogic Server. It might be necessary to re-create the WAR or WAR and EAR files before you deploy.



### “Re-creating the WAR or EAR file”

Any time that you make changes to 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 Application Engine”

To use Workplace as a web application, you must deploy it as an application in the WebLogic Server Administration 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 make changes to 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
UNIX	<i>AE_install_path</i> /deploy/ create_app_engine_war.sh
Windows	<i>AE_install_path</i> \deploy\ create_app_engine_war.bat

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 will generate the following context root: `http://server_name:port# /app_engine`. Renaming the WAR file Workplace.war will generate 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 will by default create 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
UNIX	<i>AE_install_path</i> /deploy/ create_app_engine_ear.sh
Windows	<i>AE_install_path</i> \deploy\ create_app_engine_ear.bat

## Deploying Application Engine

To use Workplace as a web application, you must deploy it as an application in the WebLogic Server Administration Console. You can specify the context root for the application URL during the deployment.

1. From the WebLogic Administration Console, navigate to the domain you initially created for the Application Engine.
2. Prepare the WebLogic Administration Console to deploy the application.
3. Choose whether to deploy from an exploded folder (*AE\_install\_path*) or from the WAR or EAR file (default: *app\_engine.war* or *app\_engine.ear* in *AE\_install\_path/deploy*).
4. Accept the defaults for the deployment, except for the name for the deployment. Use "Workplace" instead of "appengine".
5. Finish the deployment, and save and activate your changes.

**Tip:** To verify that the deployment was successful, expand **Web Applications**. The web application Workplace is listed.

**Tip:** To troubleshoot the deployment, check the following log:

```
WLS_install_path/user_projects/domains/domain_name/servers/server_name/
logs/server_name.log
```

6. After deployment is complete, start Workplace (or your custom application name) in the WebLogic Server Administration Console.

## Deploying Application Engine on JBoss Application Server

After you install and configure Application Engine, you must deploy your client application, Workplace, on your JBoss Application Server. It might be necessary to re-create the WAR or WAR and EAR files before you deploy.

“Re-creating the WAR or EAR file”

Any time that you make changes to 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 and starting Application Engine” on page 485

To use Workplace as a web application, you must deploy it as an application on the JBoss Application Server.

### Re-creating the WAR or EAR file

Any time that you make changes to 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
UNIX	<i>AE_install_path/deploy/create_app_engine_war.sh</i>
Windows	<i>AE_install_path\deploy\create_app_engine_war.bat</i>

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* will generate the

following context root: `http://server_name:port# /app_engine`. Renaming the WAR file `Workplace.war` will generate 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 will by default create 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
UNIX	<code>AE_install_path/ deploy/ create_app_engine_ear.sh</code>
Windows	<code>AE_install_path\ deploy\ create_app_engine_ear.bat</code>

## Deploying and starting Application Engine

To use Workplace as a web application, you must deploy it as an application on the JBoss Application Server.

1. Stop the JBoss Application Server, if it is running.
2. Deploy the Workplace application: To deploy from exploded directory
  - a. On the JBoss Application Server, copy the `/Workplace` folder from:
 

```
AE_install_path
```

 to:
 

```
JBOSS_home/server/servername/deploy/
```
  - b. Append the extension `.war` to the Workplace folder:
 

```
JBOSS_home/server/servername/deploy/Workplace.war
```

 To deploy from a WAR file  
 On the JBoss Application Server, copy the `app_engine.war` file from:
 

```
AE_install_path/deploy
```

 to:
 

```
JBOSS_home/server/servername/deploy/
```

 To deploy from an EAR file  
 On the JBoss Application Server, copy the `app_engine.ear` file from:
 

```
AE_install_path/deploy
```

 to:
 

```
JBOSS_home/server/servername/deploy/
```
3. Set permissions for the user running the application server.  
 If the user that will be running the application server is different from the user that installed Application Engine, you must give the user read/write permissions on the following folders:
 

```
JBOSS_home/server/default/deploy/app_engine.war/ .ear
```

```
AE_install_path
```

 For Windows this is only required for NTFS formatted partitions.
4. Start the JBoss Application Server.
5. Verify that the application deployed successfully.

Verify that the `server.log` file located in `JBOSS_home/server/servername/log` lists deployment of the WAR or EAR file you used.

---

## Completing post-upgrade Application Engine configuration

After you upgrade and deploy your Application Engine instances, you can complete additional configuration. Actions include modifying a configuration file, verifying Workplace sign-in, and establishing the Process Engine connection point.

To complete post-upgrade Application Engine configuration:

1. (WebLogic Server only) If you upgraded from WebLogic Server 8.1 to WebLogic Server 9 or 10, you must set the case-sensitivity for the server.
  - a. From the WebLogic Server Administration Console, click **my\_domain**.
  - b. Set **Web App Files Case Insensitive** to false.
  - c. Save and activate your changes.
2. If it is not already running, start the Workplace application on your application server.
3. Sign in to Workplace to test your connection.
  - a. On any computer, open a browser and type: `http://server_name:port#/Workplace`
  - b. Enter a user name and password, and click **Sign in**.
4. Set the Process Engine Connection Point.

The Process Router from version 3.5 has been replaced with the Application Engine Connection Point.

  - a. In Workplace click **Admin**.
  - b. Click **Site Preferences**.
  - c. Under **General Settings** → **Tasks**, select a **Process Engine Connection Point** from the drop down list.
  - d. Click **Apply** and then **Exit**.
  - e. Confirm that Application Engine is communicating with Process Engine.
    - 1) In Workplace, click **Tasks**.
    - 2) Verify that the Tasks page displays.
  - f. Sign out of Workplace.

---

## Upgrading add-on components

You must upgrade all of the IBM FileNet P8 Platform core components before upgrading the add-on components listed in this topic.

See Part 2, “Upgrading and configuring IBM FileNet P8 Platform,” on page 205 for the tasks required to upgrade the IBM FileNet P8 Platform core components.

You can upgrade the add-on components in the following list, and any IBM FileNet P8 Platform expansion products, in any order, except that you must upgrade Process Analyzer before upgrading Process Simulator.

For details and procedures on updating add-on components, see the following topics:

“Upgrading Application Integration and File Tracker”

Upgrading to Workplace Application Integration 4.0.2 involves installing the a new version on top of your existing Workplace Application Integration 3.5 or 4.0 install. The upgrade installation program detects the earlier version and notifies you before proceeding with the upgrade.

“Upgrading IBM FileNet publishing components” on page 489

If you have IBM FileNet Rendition Engine software currently installed, you can upgrade to the latest software version.

“Upgrading server-side scripts and COM objects” on page 489

As with version 3.5 of Content Engine, you can develop and plug in the following server-side components for version 4 of Content Engine: event action handlers, lifecycle action handlers, and document classifiers.

“Upgrading Image Services Resource Adapter servlet” on page 494

To upgrade the Image Services Resource Adapter software, you must upgrade Application Engine and ensure that existing Image Services Resource Adapter is installed and configured.

---

## Upgrading Application Integration and File Tracker

Upgrading to Workplace Application Integration 4.0.2 involves installing the a new version on top of your existing Workplace Application Integration 3.5 or 4.0 install. The upgrade installation program detects the earlier version and notifies you before proceeding with the upgrade.

During the upgrade, the installer detects the Microsoft applications that were previously integrated with Workplace and retains that configuration. For example, if you had Microsoft Outlook integrated with Workplace in the 3.5 release, Microsoft Outlook integration is upgraded to 4.0.2 during the upgrade installation.

You cannot change your installed components during the upgrade. You can add or remove a Microsoft application from Application Integration after the upgrade using your Add/Remove Programs application.

Verify your computer meets the platform requirements documented in the *IBM FileNet P8 Hardware and Software Requirements*.

Consider the following upgrade scenarios:

- If you upgrade from Application Integration version 3.5.1-001 or earlier, the upgrade to 4.0.2 will install File Tracker for you.
- If you upgrade from Application Integration version 3.5.1-002 or higher, then these conditions apply:
  - If you only had Application Integration installed (without File Tracker), then the upgrade to 4.0.2 will install File Tracker for you.
  - If you had both Application Integration and File Tracker installed, then the order in which you installed these applications determines your upgrade path.
    - If you installed File Tracker 3.5.1-002 or higher before you installed Application Integration, you must upgrade File Tracker before you upgrade Application Integration.
    - If you installed Application Integration 3.5.1-002 or higher, and later used File Tracker, upgrade Application Integration.

“Upgrading Workplace Application Integration”

The Workplace Application Integration installation program detects your installation, and upgrades the application to version 4.0.2. To run the installation program, you must have Administrator privileges.

“Verify your Workplace Application integration upgrade” on page 489

To verify your Workplace Application integration upgrade, you can use Microsoft Word to view the Workplace address and the version number.

“Upgrading Workplace File Tracker” on page 489

The Workplace File Tracker installation program detects your installation, and upgrades the application to version 4.0.2. To run the installation program, you must have Administrator privileges.

## Upgrading Workplace Application Integration

The Workplace Application Integration installation program detects your installation, and upgrades the application to version 4.0.2. To run the installation program, you must have Administrator privileges.

To upgrade Application Integration:

1. To obtain the latest component software updates, and to determine whether additional interim fixes are needed, contact your service representative.
2. Open the readmes for the software updates and perform the installation procedures in the readmes on the component machine.
3. On the client machine that has Application Integration installed, log in with an account that has Administrator privileges.
4. Sign in to Workplace.
5. Click **Author**, and then click **General Tools**.
6. Click **Download Application Integration for Microsoft Office**. The File Download dialog box for your system appears. Do one of the following steps:
  - 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 upgrade installer.

If you have Workplace Application Integration 3.5 currently installed, the installer prompts you about the upgrade. Click **Yes** to upgrade to the current version you are installing or click **No** to end the installation.

7. After the install is complete, click **Finish** to complete the upgrade process.

## Verify your Workplace Application integration upgrade

To verify your Workplace Application integration upgrade, you can use Microsoft Word to view the Workplace address and the version number.

To verify the upgrade:

1. Start Microsoft Word.
2. Click **File** → **FileNet P8** → **Open Document** → **Select Item**. The Logon dialog box opens.
3. Log on with any valid domain account.
4. Click **Options** to view the Workplace address. The version number appears below the address.
5. Close all dialog boxes and close Microsoft Word.

## Upgrading Workplace File Tracker

The Workplace File Tracker installation program detects your installation, and upgrades the application to version 4.0.2. To run the installation program, you must have Administrator privileges.

To upgrade File Tracker:

1. To obtain the latest component software updates, and to determine whether additional interim fixes are needed, contact your service representative.
2. Open the readmes for the software updates and perform the installation procedures in the readmes on the component machine.
3. On the client machine where File Tracker is installed, log on with an account that has Administrator privileges.
4. Sign in to Workplace.
5. Click **Author**, and then click **General Tools**.
6. Scroll down and click **Download File Tracker** and do one of the following steps:
  - 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 FileTracker.exe file locally. Then click **Save**. After the file is saved to your hard drive, double-click the file to run the upgrade installer.
7. After the install is complete, click **Finish** to complete the upgrade process.

---

## Upgrading IBM FileNet publishing components

If you have IBM FileNet Rendition Engine software currently installed, you can upgrade to the latest software version.

For instructions, see the *IBM FileNet Rendition Engine Installation and Upgrade Guide* at *FileNet P8 Documentation > FileNet P8 System Installation > Rendition Engine Installation and Upgrade*.

---

## Upgrading server-side scripts and COM objects

As with version 3.5 of Content Engine, you can develop and plug in the following server-side components for version 4 of Content Engine: event action handlers, lifecycle action handlers, and document classifiers.



Whereas these components had to be implemented as COM objects or scripts for version 3.5 of Content Engine, they must be implemented as Java classes in version 4 of Content Engine. Therefore, for version 4, you must convert any event action handlers, lifecycle action handlers, and document classifiers that you developed for version 3.5.

You need to know the amount of effort involved in converting version 3.5 script-based event action handlers to version 4 Java-implemented handlers. For details on developing and deploying event action handlers, lifecycle action handlers, and document classifiers, see the Java and .NET Developer's Guide and the Java API Reference.

Compare listings of the version 3.5 script-based event action handlers to the corresponding Java-implemented handlers required for version 4 of Content Engine

“File document handler”

This handler files a document to a specified folder, determined by the event fired on the document.

“Log event handler” on page 491

This handler records events to a log file when documents are created.

“Send eMail handler” on page 493

This handler sends an email when a new document has been created.

## File document handler

This handler files a document to a specified folder, determined by the event fired on the document.

File document handler
Content Engine 3.5.x JScript Version
<pre>function OnEvent (Event, Subscription) { var doc = Event.SourceObject; if (Event.IsOfClass("CreationEvent")) { FileDocInFolder("/Docs", doc); } else if (Event.IsOfClass("ChangeClassEvent")) { FileDocInFolder("/Archives", doc); } } function FileDocInFolder(otherFolderName, doc) { var os = doc.ObjectStore; var rootFld = os.RootFolder; var fldSet = new Enumerator(rootFld.SubFolders); var subFld; for (; !fldSet.atEnd(); fldSet.moveNext()) { subFld = fldSet.item(); if (subFld.Name == otherFolderName) { subFld.File(doc, 0, doc.DocumentTitle); } } }</pre>
Content Engine 4.x Java Version

### File document handler

```
import com.filenet.api.constants.*;
import com.filenet.api.constants.DefineSecurityParentage;
import com.filenet.api.core.*;
import com.filenet.api.engine.EventActionHandler;
import com.filenet.api.events.ObjectChangeEvent;
import com.filenet.api.exception.EngineRuntimeException;
import com.filenet.api.exception.ExceptionCode;
import com.filenet.api.util.Id; public class FileDocumentAction implements
EventActionHandler {

public void onEvent(ObjectChangeEvent event, Id subscriptionId) throws
EngineRuntimeException
{
Document doc = (Document)event.get_SourceObject();
try
{
if (event.getClassName().equalsIgnoreCase("CreationEvent"))
FileDocInFolder("/docs", doc);
else if (event.getClassName().equalsIgnoreCase("ChangeClassEvent"))
FileDocInFolder("/Archives", doc);
}
catch (Exception e)
{
throw new EngineRuntimeException(ExceptionCode.E_FAILED);
}
}

public void fileDocInFolder(String folderName, Document doc)
{
try
{
Folder folder = (Folder)doc.getObjectStore().getObject("Folder", folderName);
ReferentialContainmentRelationship rel = folder.file (doc,
AutoUniqueName.AUTO_UNIQUE, doc.get_Name(),
DefineSecurityParentage.DO_NOT_DEFINE_SECURITY_PARENTAGE);
rel.save(RefreshMode.NO_REFRESH);
}
catch (Exception e)
{
e.printStackTrace();
}
}
}
```

## Log event handler

This handler records events to a log file when documents are created.

### Log event handler

Content Engine 3.5.x VBScript Version

### Log event handler

```
Public Sub OnEvent (EventObject, Subscription)
Dim doc, message)
Set doc = EventObject.SourceObject)
WriteToLogFile (doc.Name & " was created on: " & Date))
End Sub
```

```
Public Sub WriteToLogFile (message))
Dim fso, ts, logFile)
Set fso = CreateObject("Scripting.FileSystemObject")
Set logFile = fso.CreateTextFile("C:\\log.txt")
logFile = nothing)
Set ts = fso.OpenTextFile("C:\\log.txt", 8, True))
ts.Write (message))
ts.WriteBlankLines (2))
ts.Close)
Set fso = Nothing)
Set ts = Nothing)
End Sub
```

### Content Engine 4.x Java Version

```
import java.io.File;
import java.io.FileWriter;
import java.io.IOException;

import com.filenet.api.core.Document;
import com.filenet.api.engine.EventActionHandler;
import com.filenet.api.events.ObjectChangeEvent;
import com.filenet.api.exception.EngineRuntimeException;
import com.filenet.api.exception.ErrorRecord;
import com.filenet.api.exception.ExceptionCode;
import com.filenet.api.util.Id;

public class LogEventAction implements EventActionHandler
{
public void onEvent(ObjectChangeEvent event, Id subscriptionId) throws
EngineRuntimeException
{
try
{
Document doc = (Document)event.get_SourceObject();
WriteToLogFile(doc.get_Name()
+ " was created on: " + new java.util.Date() + "\r\n");
}
catch (Exception e) {
ErrorRecord er[] = {new ErrorRecord (e)};
throw new EngineRuntimeException(e, ExceptionCode.EVENT_HANDLER_THREW, er);
}
}

public void writeToLogFile(String message)
{
try
{
File outputFile = new File("C:\\\\log.txt");
FileWriter out = new FileWriter(outputFile, true);
out.write(message);
out.close();
}
catch (IOException e) {
ErrorRecord er[] = {new ErrorRecord (e)};
throw new EngineRuntimeException(e, ExceptionCode.EVENT_HANDLER_THREW,er);
}
}
}
```

## Send eMail handler

This handler sends an email when a new document has been created.

Send email handler
Content Engine 3.5.x VBScript Version
<pre>Public Sub OnEvent (EventObject, Subscription) Dim myMail, MessageBody Set myMail = CreateObject("CDONTS.NewMail") myMail.From = "user1@company.com" myMail.To = "sysAdmin@company.com" myMail.Subject = "Event Notification--New Document created" MessageBody = "A document titled "" &amp; Source.DocumentTitle &amp; "" was Created at " &amp; time &amp; " on " &amp; date &amp; "." MessageBody = MessageBody + vbCrLf + Subscription.UserString myMail.Body = MessageBody myMail.Send Set myMail = Nothing End Sub</pre>
Content Engine 4.x Java Version

### Send email handler

```
import java.util.Date;
import java.util.Properties;

import javax.mail.Message;
import javax.mail.MessagingException;
import javax.mail.Session;
import javax.mail.Transport;
import javax.mail.internet.InternetAddress;
import javax.mail.internet.MimeMessage;

import com.filenet.api.core.*;
import com.filenet.api.engine.EventActionHandler;
import com.filenet.api.events.ObjectChangeEvent;
import com.filenet.api.exception.EngineRuntimeException;
import com.filenet.api.exception.ExceptionCode;
import com.filenet.api.util.Id;

public class EMailAction implements EventActionHandler
{
 public void onEvent(ObjectChangeEvent event, Id subscriptionId) throws
 EngineRuntimeException
 {
 Document doc = (Document)event.get_SourceObject();
 try
 {
 Properties props = new Properties();
 props.put("mail.smtp.host", "smtp.company.net");
 props.put("mail.smtp.port", "25");
 Session session = Session.getInstance(props);
 try {
 Message msg = new MimeMessage(session);
 msg.setFrom(new InternetAddress("user1@company.com")); InternetAddress[]
 address = {new InternetAddress("sysAdmin@company.com")};
 msg.setRecipients(Message.RecipientType.TO, address);
 msg.setSubject("Test E-Mail through Java");
 msg.setSentDate(new Date());
 msg.setText("Document " + doc.get_Name() + " created with ID " + doc.get_Id());
 Transport.send(msg);
 }
 catch (MessagingException mex) {
 mex.printStackTrace();
 }
 }
 catch (Exception e)
 {
 throw new EngineRuntimeException(ExceptionCode.E_FAILED);
 }
 }
}
```

---

## Upgrading Image Services Resource Adapter servlet

To upgrade the Image Services Resource Adapter software, you must upgrade Application Engine and ensure that existing Image Services Resource Adapter is installed and configured.

As part of upgrading Image Services Resource Adapter (ISRA) software to run with IBM FileNet P8, you must verify the following prerequisites have been completed:

- Ensure that Application Engine has been upgraded.
- Ensure that existing Image Services Resource Adapter software is installed and configured.

For information on installing, configuring, and deploying FileNet ISRA, See the ISRA documentation on the IBM FileNet ISRA installation package.

**Tip:** Use the Sample Application shipped with IBM FileNet ISRA to confirm that the ISRA installation was successful.

**Attention:** In an ISRA upgrade, take care to use the same library name (JNDI connection factory name) that has been previously set in the ISRA install. Changing this variable can cause conflicts when accessing documents.

- Do the following tasks:
  - Upgrade the Application Engine ISRA Servlet, taking the following into account:
    - The servlet must be deployed on the same application server as FileNet ISRA.
    - The servlet does not need to be collocated with the Application Engine.
  - Configure Workplace site preferences for ISRA support.

“ISRA SSL support”

ISRA support for SSL depends upon the configuration, including the location where the ISRA Servlet and Application Engine are installed, and whether the ISRA Servlet and Application Engine are currently running under SSL.

“Upgrading the Application Engine Image Services Resource Adapter servlet” on page 496

To upgrade the Application Engine IBM FileNet Image Services Resource Adapter (ISRA) servlet, you must run its installation program. You must also complete additional configuration and deployment steps.

“Configuring the Workplace site preferences for ISRA support” on page 498

Before you can access IBM FileNet Image Services libraries from Workplace, you must configure the site preferences in Workplace.

“Setting the ISRA interface servlet URL” on page 498

To enable ISRA support for SSL, you must define the URL of the ISRA interface servlet.

“Logging on to Image Services through LDAP” on page 498

To log on to Image Services through LDAP, you must first configure ISRA and Image Services for LDAP authentication.

“Accessing IS library documents” on page 499

Before you can access IS library documents, you must use Workplace to add these documents to an object store.

“Installing component software updates” on page 499

You must apply any available updates, fix packs, or interim fixes for the component software.

## ISRA SSL support

ISRA support for SSL depends upon the configuration, including the location where the ISRA Servlet and Application Engine are installed, and whether the ISRA Servlet and Application Engine are currently running under SSL.

The following table shows the supported SSL configurations.

SSL Configuration	SSL Support
ISRA Servlet and AE Collocated. AE configured for SSL logon redirect to a non-local host.	Supported
ISRA Servlet and AE Collocated. AE configured for SSL logon redirect to a local host.	Supported
ISRA Servlet and AE Collocated. AE and ISRA Servlet running under SSL.	Not Supported
ISRA Servlet remote from AE. AE configured for SSL logon redirect to a non-local host.	Supported
ISRA Servlet remote from AE. AE configured for SSL logon redirect to a local host.	Supported
ISRA Servlet remote from AE. AE running under SSL, ISRA Servlet not running under SSL.	Supported
ISRA Servlet remote from AE. AE and ISRA Servlet running under SSL.	Not Supported

## Upgrading the Application Engine Image Services Resource Adapter servlet

To upgrade the Application Engine IBM FileNet Image Services Resource Adapter (ISRA) servlet, you must run its installation program. You must also complete additional configuration and deployment steps.

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

The Application Engine installation packages contain the ISRA servlet installation programs for the supported Application Engine platforms.

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 Application Engine ISRA servlet values, filter by **ISRA Installer** in the **Installation or Configuration Program** column.

2. Log on to the application server machine:

Option	Description
<b>UNIX</b>	Log on as a user with write access to the /bin directory and read, write, execute access to the directory where you plan to install ISRA servlet.
<b>Windows</b>	Log on as a member of the local Administrators group or as a user with equivalent permissions.

3. (WebSphere Application Server and WebLogic Server only) Back up and undeploy the ISRA servlet application on the application server.
4. Stop the application server if it is running.
5. (JBoss Application Server only) Back up and undeploy the ISRA servlet application.



6. Access the Application Engine ISRA installation package.
7. Start the Application Engine ISRA servlet installation program, which is also covers upgrades:

Option	Description
UNIX	AE-ISRA-Servlet-4.0.2.0-operating_system.bin
Windows	AE-ISRA-Servlet-4.0.2.0-WIN.exe

8. Complete the installation program screens by using the values in your worksheet.
9. 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.
10. Install unlimited strength jar files.  
Perform this step only if your site is generating or accepting unlimited strength user tokens. Your system must be configured as follows:
  - The Application Engine ISRA servlet is deployed on a different application server from the Application Engine server.
  - The Create unlimited strength key option was selected in the Application Engine User Token Security step of the Application Engine installation.
 If you do not install the unlimited strength jar files, and your site generates or accepts unlimited strength user tokens, cause an `EncryptionException` occurs when you log in to the IS Server.
11. (WebSphere Application Server and WebLogic Server only) Start the application server.
12. Deploy `AE_israservlet_install_path/FileNet/ApplicationEngineISRAServlet/ae_isra.war` in the same way you deployed the `app_engine.war` file for Workplace.
13. (JBoss Application Server only) Start the application server.
14. Verify the Application Engine ISRA servlet installation. Do the following to use an available diagnostic tool to verify that the ISRA servlet is installed and deployed correctly.

a. Launch your 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 installed and deployed 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 concepts

 Installation and Upgrade Worksheet

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

## Configuring the Workplace site preferences for ISRA support

Before you can access IBM FileNet Image Services libraries from Workplace, you must configure the site preferences in Workplace.

Application Engine Setup installs a pre-configured external service called Image Service, which includes the parameterized values necessary to access Image Services libraries from Workplace. Enable the service by setting the *Image Service* value in Site Preferences to *Show* (the default is *Hide*), as described in the following procedure.

1. Sign in to Workplace as a user having the Application Engine Administrators access role.
2. Launch Site Preferences as follows:
  - a. Click **Admin**.
  - b. Click **Site Preferences**.
3. Click **External Services** from the left options list.
4. Click **Modify** for the Image Service (under External Reference Services).  
The External Reference Service Settings site preference page displays.
5. Under General Information, locate *Show on Select File page* and change the value to Show.
6. Click **Accept**.
7. Click **Apply**.

## Setting the ISRA interface servlet URL

To enable ISRA support for SSL, you must define the URL of the ISRA interface servlet.

1. Click **Bootstrap**.
2. 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.

3. Click **Apply**.
4. Click **Exit** to exit the Site Preferences.

## Logging on to Image Services through LDAP

To log on to Image Services through LDAP, you must first configure ISRA and Image Services 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 Image Services, see the *Image Services System Tools Reference Manual*.

To log on to the Image Services library with your LDAP account, configure ISRA and Image Services for LDAP authentication. If the LDAP account with which you accessed Workplace is not valid for the Image Services library, or if LDAP authentication is not configured, you will be prompted to log on to the Image Services library.

## Accessing IS library documents

Before you can access IS library documents, you must use Workplace to add these documents to an object store.

For information about accessing IS library documents, see IBM FileNet P8 Help topic **User Help** → **Actions, preferences and tools** → **Actions** → **Documents** → **Add a document (Workplace)**.

## Installing component software updates

You must apply any available updates, fix packs, or interim fixes for the component software.

1. To obtain the latest component software updates, and to determine whether additional interim fixes are needed, contact your service representative.
2. Open the readmes for the software updates and perform the installation procedures in the readmes on the component machine.



---

## Part 3. Removing software

Removing IBM FileNet P8 software can involve deleting one or more core components, expansion products, and the FileNet P8 documentation.

For instructions on removing the Rendition Engine software, see the IBM FileNet P8 guide *FileNet P8 Documentation > FileNet P8 System Installation > Rendition Engine Installation and Upgrade*.

“Removing the IBM FileNet P8 documentation” on page 503

Removing the documentation for the FileNet P8 Platform and its expansion products involves a number of application server configuration possibilities. Use these examples only for reference. Your specific installation directories and application names might vary.

“Removing Content Engine” on page 505

You can uninstall an entire Content Engine installation or selected Content Engine components.

“Removing Content Search Engine” on page 507

To completely remove 4.5 Content Search Engine (Autonomy K2) and collections from your IBM FileNet P8 Platform installation, you must disable full-text indexing. You must also remove the Autonomy K2 installations from all servers associated with the Content Engine.

“Removing additional locales (UNIX)” on page 509

Remove the additional locales that you installed on UNIX machines.

“Removing additional locales (Windows)” on page 511

Remove the additional locales that you installed on Windows machines.

“Removing Process Engine (Windows)” on page 513

Removal of the Process Engine for Windows platforms requires that you remove the software components in a specific order.

“Removing Process Engine (UNIX)” on page 515

Removal of the Process Engine on UNIX platforms requires that you stop IBM FileNet P8 software components and run specific commands.

“Removing Application Engine (WebSphere)” on page 517

Removal of the Application Engine for WebSphere on UNIX and Windows platforms requires that you log on to the application server and run the uninstall program.

“Removing Application Engine (WebLogic)” on page 519

Removal of the Application Engine for WebLogic on UNIX and Windows platforms requires that you log on to the application server and run the uninstall program.

“Removing Application Engine (JBoss Application Server)” on page 521

Removal of the Application Engine for JBoss Application Server on UNIX and Windows platforms requires that you log on to the application server and run the uninstall program.

“Removing the Application Engine ISRA servlet” on page 523

Removal of the Application Engine ISRA Servlet for Windows and UNIX environments requires that you log on to the application server, undeploy the servlet, and run the uninstall program.

“Removing Workplace Application Integration” on page 525

You can remove Application Integration by using the Microsoft Windows Control Panel, or you can remove the program files silently from the command line.

“Removing Workplace File Tracker” on page 527

You can remove File Tracker by using the Microsoft Windows Control Panel, or you can remove the program files silently from the command line.

---

## Removing the IBM FileNet P8 documentation

Removing the documentation for the FileNet P8 Platform and its expansion products involves a number of application server configuration possibilities. Use these examples only for reference. Your specific installation directories and application names might vary.

In some Windows installations where NTFS is used for the file system (Not FAT or FAT32), there is a known issue with deleting files (and folders) that are longer than 256 characters. For example, if you use a default WebSphere installation location, you might encounter an error where the FileNet P8 Platform documentation files cannot be properly deleted due to the number of characters in the file/folder names. See the Microsoft Knowledge Base article <http://support.microsoft.com/?kbid=320081> for additional information about deleting files (and folders) in this environment.

“Removing the FileNet P8 documentation from a WebSphere Application Server”

To remove the FileNet P8 documentation, delete the entire FileNet P8 documentation folder (for example, `ecm_help.war`) structure from the installation location.

“Removing the FileNet P8 documentation from a WebLogic Server” on page 504

To remove the FileNet P8 documentation from a WebLogic Server, delete all folders and files including any temp folder(s) or log files for the FileNet P8 documentation.

“Removing the FileNet P8 documentation from a JBoss Application Server” on page 504

To remove the FileNet P8 documentation, log on to the JBoss FileNet P8 documentation server, and delete all folders and files associated with FileNet P8 documentation server.

---

## Removing the FileNet P8 documentation from a WebSphere Application Server

To remove the FileNet P8 documentation, delete the entire FileNet P8 documentation folder (for example, `ecm_help.war`) structure from the installation location.

1. Log on to the WebSphere FileNet P8 documentation server.

Option	Description
UNIX	Log on as a user with delete access to where the FileNet P8 Platform documentation files are installed.
Windows	Log on with a user account that has local Administrative (or Account Operators and Server Operators) rights.

2. Verify that the WebSphere server is running.
3. From the WebSphere administrative console (for example, `http://localhost:9060/ibm/console`), *Uninstall* the FileNet P8 documentation site (for example, `ecm_help.war`).



4. Delete the entire FileNet P8 documentation folder (for example, ecm\_help.war) structure from the installation location.
5. Delete any temp folder(s) or log files for the FileNet P8 documentation.

**Important:** Do not remove any other FileNet P8 application (for example, Workplace) files that are installed on the web application server.

---

## Removing the FileNet P8 documentation from a WebLogic Server

To remove the FileNet P8 documentation from a WebLogic Server, delete all folders and files including any temp folder(s) or log files for the FileNet P8 documentation.

1. Log on to the WebLogic Server.

Option	Description
UNIX	Log on as a user with delete access to where the ecm_help files are located.
Windows	Log on with a user account that has local Administrative rights (or Account Operators and Server Operators).

2. Verify that the WebLogic Server is running.
3. From the WebLogic Server Administration Console (for example, <http://<machinename>:7001/console>), *Delete* the FileNet P8 documentation site (for example, ecm\_help).
4. Delete all folders and files including any temp folder(s) or log files for the FileNet P8 documentation.

**Important:** Do not remove any other FileNet P8 application (for example, Workplace) files that are installed on the web application server.

---

## Removing the FileNet P8 documentation from a JBoss Application Server

To remove the FileNet P8 documentation, log on to the JBoss FileNet P8 documentation server, and delete all folders and files associated with FileNet P8 documentation server.

1. Log on to the JBoss FileNet P8 documentation server.

Option	Description
UNIX	Log on as a user with delete access to where the FileNet P8 Platform documentation files are installed.
Windows	Log on with a user account that has local Administrative (or Account Operators and Server Operators) rights.

2. Stop the JBoss Application Server.
3. Delete all folders and files including any temp folder(s) or log files for the FileNet P8 documentation (for example, ecm\_help).

**Attention:** Do not remove any other FileNet P8 application (for example, Workplace) files that are installed on the web application server.

---

## Removing Content Engine

You can uninstall an entire Content Engine installation or selected Content Engine components.

Uninstalling Content Engine does not undeploy it. You must use the application server console or commands to remove the Content Engine EAR file from the application server.

Use one of the following procedures to uninstall part or all of Content Engine.

“Removing part or all of a Content Engine installation interactively by using the Windows control panel”

You can remove part or all of a Content Engine installation.

“Removing an entire Content Engine installation interactively (UNIX)”

To remove an entire Content Engine installation, navigate to the *install\_path/FileNet/ContentEngine/\_ceuninst* directory and issue the following command: `ce_uninstaller`.

“Removing Content Engine silently” on page 506

In silent mode, the uninstaller removes all Content Engine components.

“Removing data associated with Content Engine” on page 506

After uninstalling Content Engine, you can remove its associated data.

---

### Removing part or all of a Content Engine installation interactively by using the Windows control panel

You can remove part or all of a Content Engine installation.

To remove Content Engine:

1. Choose **Control Panel** → **Add/Remove Programs**.
2. Highlight P8 Content Engine in the list of currently installed programs and click **Change/Remove** to launch the Uninstall P8 Content Engine program.
3. In the Uninstall Options screen, choose to uninstall some or all Content Engine components.
4. In the Choose Components screen, choose which components to remove.
5. In the Uninstall Complete screen, note the directories and files that cannot be removed by the uninstall program and choose whether to have the program restart the machine, or restart it manually.
6. Remove the remaining directories and files, as noted in the Uninstall Complete screen.
7. If you want to completely remove all traces of the Content Engine installation, delete the `C:\Program Files\IBM\FileNet` directory.

---

### Removing an entire Content Engine installation interactively (UNIX)

To remove an entire Content 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 Engine installer.

2. To uninstall Content Engine interactively, run the following command:  
`ce_uninstaller`

---

## Removing Content Engine silently

In silent mode, the uninstaller removes all Content Engine components.

To uninstall Content Engine silently, run one of the following commands:

Option	Description
UNIX	<code>ce_uninstaller -i silent</code>
Windows	<code>ce_uninstaller.exe -i silent</code>

---

## Removing data associated with Content Engine

After uninstalling Content Engine, you can remove its associated data.

1. Use the application server console or command lines to undeploy Content Engine.
2. Use the application server console or command lines to remove any database JDNI data sources associated with Content Engine object stores. For JBoss, remove the `datasource-name-ds.xml` files.
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 *Plan and Prepare Your Environment for IBM FileNet P8*.
5. Use your operating system commands to delete any directories, users, and groups that were used for installing and administering Content 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 (K2 collections).

---

## Removing Content Search Engine

To completely remove 4.5 Content Search Engine (Autonomy K2) and collections from your IBM FileNet P8 Platform installation, you must disable full-text indexing. You must also remove the Autonomy K2 installations from all servers associated with the Content Engine.

### Important:

- If you remove or disable Autonomy K2 before you disable CBR and full-text indexing in Enterprise Manager, your system is rendered unusable and require considerable reconstruction.
- This procedure presumes you have a running installation of version 4.5 Content Search Engine and that you have existing collections.
- If you intend to remove Content Engine, skip to 4.

To remove Autonomy K2 and CBR:

1. Launch Enterprise Manager.
2. Disable CBR for any classes that have been enabled for CBR.
  - a. Right-click the class you want to configure and click **Properties**.
  - b. Click the **General** tab.
  - c. Clear the **CBR Enabled** check box and click **OK**.
  - d. A dialog asks if you want to propagate this change to the subclasses of this class. Click **Yes**.
  - e. Repeat this procedure to disable CBR for all classes.
3. Run an index job and reindex any of these objects that were previously enabled:
  - Document
  - Annotation
  - Custom Object
  - Folder

The index job disables all full-text indexing and content-based retrieval settings and deletes any associated collections. After the index job is complete, continue with the next step.
4. As *k2\_os\_user*, log on to the Master Administration Server machine in your IBM FileNet P8 Content Search Engine configuration.
5. Complete the steps in the table to remove the Autonomy K2 software on the machine.

Option	Description
Windows	<ol style="list-style-type: none"><li>1. Access the Add or Remove Programs control panel and select <b>IBM FileNet P8 Content Search Engine</b>.</li><li>2. Click <b>Change/Remove</b>.</li></ol>

Option	Description
UNIX	<ol style="list-style-type: none"> <li data-bbox="933 226 1398 373">1. Stop the Autonomy K2 Administration Server service and the Tomcat application server. Use the following command, according to your environment: <ul style="list-style-type: none"> <li data-bbox="971 390 1414 447"><b>HP-UX</b> <code>verity_install_path/k2/_hpux/bin/k2adminstop</code></li> <li data-bbox="971 464 1344 520"><b>AIX</b> <code>verity_install_path/k2/_rs6k43/bin/k2adminstop</code></li> <li data-bbox="971 537 1344 594"><b>Solaris</b> <code>verity_install_path/k2/_ssol26/bin/k2adminstop</code></li> <li data-bbox="971 611 1344 667"><b>Linux</b> <code>verity_install_path/k2/_ilnx21/bin/k2adminstop</code></li> </ul> </li> <li data-bbox="933 684 1333 741">2. Change directory to: <code>verity_install_path/_cseuninst</code></li> <li data-bbox="933 747 1292 804">3. Run the following command: <code>./CSE_uninstaller</code></li> </ol>

6. Delete `verity_install_path` on the machine.
7. Repeat 5 on page 507 and 6 for each remaining machine in your IBM FileNet P8 Content Search Engine configuration.

---

## Removing additional locales (UNIX)

Remove the additional locales that you installed on UNIX machines.

To remove locales:

1. Change your current directory to *verity\_install\_path/k2*.
2. To remove all single-language locales, run the following command: `_uninst_loc`
3. To remove all European locales, run the following command: `_uninst_eur`





---

## Removing additional locales (Windows)

Remove the additional locales that you installed on Windows machines.

To remove locales:

1. Click **Start** → **Add or Remove Programs**.
2. To remove all single-language locales, select **Verity Locales 6.1**. Then right-click, and select **Uninstall**.
3. To remove all European locales, select **Verity Single-Language European Locales 6.1**. Then right-click and select **Uninstall**.



---

## Removing Process Engine (Windows)

Removal of the Process Engine for Windows platforms requires that you remove the software components in a specific order.

**Important:** You must remove the software in the order listed. If you remove Image Services before you remove Process Engine, the Process Engine software will be left in a state that will not allow removal with this procedure.

To remove the Process Engine software:

1. Stop all of the following components that are running. For procedures and further details, see the IBM FileNet P8 help topic **System Administration** → **Enterprise-wide Administration** → **Shutdown and Startup**.

Component	Server
Process Simulator	Process Simulator
Process Analyzer	Process Analyzer
Component Manager	Application Engine
Application Engine	Application Engine
Content Engine	Content Engine
Process Service	Process Engine
Process Task Manager	Process Engine or Application Engine

2. Navigate to **Control Panel** → **Add/Remove Programs**.
3. Click **Remove** for the Process Engine application.
4. Click **Next** at the Welcome screen for Process Engine uninstallation.
5. Click **Next** to stop FileNet BPM software components.
6. Click **Uninstall** to confirm you want to remove Process Engine for Windows 4.5.0 installation.
7. Indicate whether you want to reboot now or later.
8. Click **Finish** after you've read the summary information.
9. Click **Remove** for the Image Services 4.1.2 software.
10. Enter Yes to confirm you want to remove the Image Services software.
11. Press Enter to continue with the removal.
12. Close the Add/Remove snap-in.
13. Close the Control Panel.

**Important:** (Microsoft SQL Server only) If you plan to reinstall Process Engine and will configure Process Engine to use a different SQL Server database, you must remove the database that was configured for the Process Engine installation. In addition, you must remove the following FileNet user IDs from the SQL Server Security folder before you reinstall Process Engine software:

- f\_sw
- f\_maint



---

## Removing Process Engine (UNIX)

Removal of the Process Engine on UNIX platforms requires that you stop IBM FileNet P8 software components and run specific commands.

To remove the Process Engine software:

1. Stop all of the following components that are running. For procedures and further details, see the IBM FileNet P8 help topic [System Administration > Enterprise-wide Administration > Shutdown and Startup](#).

Component	Server
Process Simulator	Process Simulator
Process Analyzer	Process Analyzer
Component Manager	Application Engine
Application Engine	Application Engine
Content Engine	Content Engine
Process Service	Process Engine
Process Task Manager	Process Engine or Application Engine

2. Enter the following after the FileNet software is shut down:

```
killfns -A -D -y
```

3. Log on to the Process Engine server as the root user.

4. On AIX, run the following command:

```
slibclean
```

5. If the `/fnsw/_pws_uninst2` directory exists, run the following command:

```
/fnsw/_pws_uninst2/pws_uninstall.bin
```

Otherwise run the following command:

```
/fnsw/_pws_uninst/pws_uninstall.bin
```

6. Follow the prompts on the screen to remove the Process Engine software.

7. At a command prompt, run the following script:

```
/fnsw/etc/uninstall
```

The uninstall script shuts down the Process Engine software, removes the software from the `/fnsw` directory, and removes the directory structure under `/fnsw`. The uninstall script removes the Process Engine entries in the `/etc/services`, `/etc/system`, `/etc/inittab` and `/etc/devlink.tab` files.

On an AIX-based Process Engine, the script also removes smit entries.



---

## Removing Application Engine (WebSphere)

Removal of the Application Engine for WebSphere on UNIX 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
UNIX	Log on as a user with read, write, and execute access to the directory where Application Engine is installed.
Windows	Log on as a member of the local Administrators group or a user with equivalent permissions.

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
UNIX	<code>uninstaller.bin</code>
Windows	<code>uninstaller.exe</code>

**Tip:** For Windows, you can also use Add/Remove Programs from the Control Panel to remove the FileNet Application Engine.

On Windows, when you click *Next* on the Application Engine Uninstaller Welcome screen, the second screen asks you to wait while Windows Task Manager service shuts down before continuing the uninstall. This can take a few moments. Wait for the shutdown to complete, then complete the uninstall wizard from the next screen.

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. (UNIX) 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 Application Engine (WebLogic)

Removal of the Application Engine for WebLogic on UNIX 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
UNIX	Log on as a user with read, write, and execute access to the directory where Application Engine is installed.
Windows	Log on as a member of the local Administrators group or a user with equivalent permissions.

2. Undeploy the Workplace application.
  - a. Stop the Workplace Web Application Module.
  - b. Delete the Workplace Web Application Module.
3. Navigate to the `/_uninst` folder under the Application Engine installation location.
4. Run the uninstall program:

Option	Description
UNIX	<code>uninstaller.bin</code>
Windows	<code>uninstaller.exe</code>

**Tip:** For Windows, you can also use Add/Remove Programs from the Control Panel to remove Application Engine.

On Windows, when you click **Next** on the Application Engine Uninstaller Welcome screen, the second screen asks you to wait while Windows Task Manager service shuts down before continuing the uninstall. This can take a few moments. Wait for the shutdown to complete, then complete the uninstall wizard from the next screen.

5. Delete the `AE_install_path` directory.
6. (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.
7. (UNIX) 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.

**Important:** Do not remove the system environment variable if any other IBM FileNet P8 application is installed on the server.



---

## Removing Application Engine (JBoss Application Server)

Removal of the Application Engine for JBoss Application Server on UNIX 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
UNIX	Log on as a user with read, write, and execute access to the directory where Application Engine is installed.
Windows	Log on as a member of the local Administrators group or a user with equivalent permissions.

2. Shut down JBoss Application Server.
3. Navigate to the /\_uninst folder under the Application Engine installation location.
4. Run the uninstall program:

Option	Description
UNIX	uninstaller.bin
Windows	uninstaller.exe

**Tip:** For Windows, you can also use Add/Remove Programs from the Control Panel to remove Application Engine.

On Windows, when you click **Next** on the Application Engine Uninstaller Welcome screen, the second screen asks you to wait while Windows Task Manager service shuts down before continuing the uninstall. This can take a few moments. Wait for the shutdown to complete, then complete the uninstall wizard from the next screen.

5. (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.
6. (UNIX and LINUX) 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.

**Important:** Do not remove the system environment variable if any other IBM FileNet P8 application is installed on the server.

7. Remove temporary files and directories.
  - a. Remove the Workplace.war folder from `JBoss_HOME\server\default\deploy\`.
  - b. Remove the Temp working directory for Workplace from `JBoss_HOME\server\server_name\work\MainEngine\localhost\`

8. Delete the *AE\_install\_path* directory.

---

## Removing the Application Engine ISRA servlet

Removal of the Application Engine ISRA Servlet for Windows and UNIX environments requires that you log on 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
UNIX	Log on as a user with write access to the directory where ISRA Servlet is installed.
Windows	Log on as a user with Administrative rights.

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"><li>1. Stop the ApplicationEngineISRAServlet process in the Admin console.</li><li>2. Uninstall the ApplicationEngineISRAServlet application from Enterprise Applications.</li></ol>
Oracle WebLogic Server	<ol style="list-style-type: none"><li>1. Stop the ApplicationEngineISRAServlet Web Application Module.</li><li>2. Undeploy or delete the ApplicationEngineISRAServlet Web Application Module.</li></ol>
JBoss Application Server	Shut down JBoss.

3. Navigate to the `/_uninstISRA` directory under the ISRA Servlet installation location.
4. Run the uninstall program:

Option	Description
UNIX	<code>uninstall.bin</code>
Windows	<code>uninstall.exe</code>

**Tip:** For Windows, you can also use Add/Remove Programs from the Control Panel to remove the FileNet Application Engine ISRA Servlet.

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\



---

## Removing Workplace Application Integration

You can remove Application Integration by using the Microsoft Windows Control Panel, or you can remove the program files silently from the command line.

“Removing or modifying Workplace Application Integration interactively”  
You can use Microsoft Windows Control Panel to remove, repair, or modify Workplace Application Integration.

“Removing Workplace Application Integration silently”

To silently uninstall Workplace Application Integration run `msiexec.exe /X{35907B7D-02E2-490C-8F3B-54C4E3729D90} /qn` at the command line.

---

### Removing or modifying Workplace Application Integration interactively

You can use Microsoft Windows Control Panel to remove, repair, or modify Workplace Application Integration.

To remove Application Integration:

1. Select **Start** → **Settings** → **Control Panel** → **Add/Remove Programs** → **FileNet Workplace Application Integration 4.0**.

2. Select the operation to perform:

- Click **Remove**, and then click **Yes** to confirm you want to uninstall Workplace Application Integration.
- Click **Change** to access maintenance tasks, and then click **Next**. You can modify, repair, or remove Application Integration using the maintenance tasks.

Select the task to perform:

- Select **Modify** to add or remove integration with Microsoft applications from your previous install. For example, if you have both Microsoft Office and Outlook installed, you can remove one of the applications by using this option. The Custom Setup dialog box opens, where you select the option you want to add or remove. Click **Next**, and then click **Install**. Click **Finish** to complete the process.
- Select **Repair** to re-install Workplace Application Integration to repair installation errors, and then click **Next**. Click **Install** to start the repair process. Click **Finish** to complete the process.
- Select **Remove** to remove Workplace Application Integration from your system, and then click **Next**. Click **Remove**. After the application is removed from your system, click **Finish** to complete the process.

---

### Removing Workplace Application Integration silently

To silently uninstall Workplace Application Integration run `msiexec.exe /X{35907B7D-02E2-490C-8F3B-54C4E3729D90} /qn` at the command line.

1. Open a command prompt.

2. Enter the following command to uninstall Workplace Application Integration:

```
msiexec.exe /X{35907B7D-02E2-490C-8F3B-54C4E3729D90} /qn
```



---

## Removing Workplace File Tracker

You can remove File Tracker by using the Microsoft Windows Control Panel, or you can remove the program files silently from the command line.

“Removing Workplace File Tracker interactively”

You can use the Microsoft Windows Control Panel to uninstall Workplace File Tracker.

“Removing Workplace File Tracker silently”

You can use a command line option to silently uninstall Workplace File Tracker.

---

### Removing Workplace File Tracker interactively

You can use the Microsoft Windows Control Panel to uninstall Workplace File Tracker.

1. From the **Start** menu, click **Settings**, and then click **Control Panel**.
2. Click **Add/Remove Programs**, and then click **FileNet Workplace File Tracker**.
3. Click **Remove**, and then click **Yes** to confirm you want to uninstall Workplace File Tracker.

---

### Removing Workplace File Tracker silently

You can use a command line option to silently uninstall Workplace File Tracker.

1. Open a command prompt.
2. Enter the following command to uninstall Workplace File Tracker:  
`msiexec.exe /X{4291FBBC-C585-43ED-9416-5F22D8C6FEE9} /qn`



---

## Part 4. Appendixes



---

## Appendix A. Configuration Manager reference

Configuration Manager is a tool for configuring and deploying new or upgraded instances of the Content Engine application on an application server.

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

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

“Overview of Configuration Manager” on page 532

You can use Configuration Manager to generate one or more unique Content Engine configuration profiles. A profile is a collection of information required to configure and deploy new or upgraded Content Engine instances.

“Handling passwords in Configuration Manager” on page 535

To provide the highest possible security, Configuration Manager's default settings 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 will must reenter passwords to run the tasks.

“Accessing the Configuration Manager log files” on page 535

Configuration Manager maintains three types of log files: the Configuration Manager session log, the Configuration Managererror log, and the task status file.

“Adding an SSL signer to the Configuration Manager keystore (WebSphere)” on page 536

If you are using SSL for communication between Content Engine 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 537

If you are using SSL for communication between Content 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 Data (GCD) or for an object store.

“Configuration Manager user interface reference” on page 538

The Configuration Manager graphical user interface (GUI) lets you create, view, and edit your Content 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 555  
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 Engine configuration profiles. A profile is a collection of information required to configure and deploy new or upgraded Content 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 534

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 Engine application.

“Gathering Configuration Manager values by using the installation and upgrade worksheet” on page 534

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 Engine is installed.

If needed, you can create multiple profiles, each of which supports a unique Content 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 Engine configuration profile:

- **Set the application server properties.** Content 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 546 or “Editing the application server properties” on page 548 for detailed procedures.

- **Configure the Java Database Connectivity (JDBC) data sources.** The JDBC data source information is used by Content Engine to connect to Global Configuration Data (GCD) and object store databases. The application server uses the JDBC data source information to connect Content 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 source task” on page 549 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 Engine application. Run this task to create the login modules on the application server.

See “Editing the configure LDAP task” on page 549 for the procedure to create the login modules after you have created a profile.

- **Configure the directory service (LDAP) provider.** Content Engine connects to the directory service provider to authenticate users. Because the application server uses the directory service information to connect the Content Engine to the directory service provider, you cannot skip this task even if you have already configured your application server prior to installing Content 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 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 549 for the procedure to set the LDAP properties after you have created a profile.

- **Configure the Content Engine bootstrap settings.** The bootstrap information is needed for creating the Global Configuration Data and for starting Content 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.

See “Editing the configure bootstrap properties settings” on page 550 for the procedure to set the bootstrap properties after you have created a profile.

- **Deploy the Content Engine application.** This action deploys the Content 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 Engine instance or update the Process Engine Client files on the Content 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 Engine application, you use Enterprise Manager to customize Content Engine for your site's requirements.

See “Editing the deploy application task” on page 550 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 554.
- **Configure a profile for upgrading an existing Content Engine from 4.** An upgrade profile includes the Upgrade Bootstrap task and the Deploy Application task. By default, the upgrade bootstrap 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 546 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 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 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 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**
- **CM: Deploy Application**
- **CM: Upgrade bootstrap**
- **CM: Upgrade Configuration Profile**

---

## Handling passwords in Configuration Manager

To provide the highest possible security, Configuration Manager's default settings 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 will 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** 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 maintains three types of log files: the Configuration Manager session log, the Configuration Managererror log, and the task status file.

- The Configuration Manager session log file. The session log contains brief information about the tasks that were run in the current session of the Configuration Manager graphical user interface (GUI). As you run additional tasks for the same or a different profile, new messages are added to the log. The messages in the session log are not time-stamped. When you exit Configuration Manager, the session log is cleared. You can view the session log from within the GUI, or you can open the session log file in a text editor:

```
ce_install_path/tools/configure/logs/P8ConfigMgr_Console.log
```

For more information about viewing the session log, see “Checking the task status” on page 554.

- The Configuration Manager error log. The error log contains details about any error occurring during execution of a task. The error messages are time-stamped, and include more information than is displayed in the session log. Unlike the session log, the error log is cumulative and contains data for more than one session. You can open the error log file in a text editor:

`ce_install_path/tools/configure/logs/P8Installer_common.log` error.

- Task status file. When you run a task in Configuration Manager, the task execution messages are displayed in the Console pane (GUI) or on the command line (CLI), and the status messages are written to a text file in the following directory:

`ce_install_path/tools/configure/profiles/myprofile/status`

The file name is based on the task that was run. You can check the status on a task at any time to review the status completion messages. For more information about checking the task status from the GUI, see “Checking the task status” on page 554. For more information about checking the task status from the CLI, see “Running Configuration Manager commands” on page 555.

---

## Adding an SSL signer to the Configuration Manager keystore (WebSphere)

If you are using SSL for communication between Content Engine 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 in the **Path** column for the truststore **NodeDefaultTrustStore**, such as `trust.p12`.
3. Start IBM Key Management by entering one of the following commands at a command prompt:

Option	Description
UNIX	<code>WAS-Home/AppServer/bin/ikeman.sh</code>
Windows	<code>WAS-Home\AppServer\bin\ikeman.bat</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 on page 536. 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 on page 536.
  - 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 Engine.
  - a. Open the DummyClientTrustFile.jks key database file located in the WebSphere profile for Content 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 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 Data (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
 -password 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 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 555.

“Starting Configuration Manager”

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

“Configuration Manager window” on page 539

The default Configuration Manager window consists of the Content 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 542

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 545

You can use the Configuration Manager commands, icons, and panes to work with your profiles and configuration tasks.

“configmgr.ini parameters” on page 555

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 Engine application instance on a web application server.

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 Engine:

Option	Description
UNIX	Run this command: <code>ce_install_path/tools/configure/configmgr</code>



Option	Description
Windows	Perform one of the following actions: <ul style="list-style-type: none"> <li>• Double-click the <b>FileNet Configuration Manager</b> desktop shortcut.</li> <li>• Click <b>Start</b> → <b>All Programs</b> → <b>IBM FileNet P8 Platform</b> → <b>FileNet Configuration Manager</b>.</li> <li>• Run the following command: <code>ce_install_path\tools\configure\configmgr.exe</code></li> </ul>

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 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.

The following table describes each pane:

Pane	Description
Content 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 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” on page 540

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 540

The Configuration Manager profile toolbar is located at the upper right of the Content Engine Task View pane. The profile toolbar contains multiple icons for working with a selected profile.

“Task toolbar” on page 541






The Configuration Manager task toolbar is located at the upper right of the Task Editor pane when a Task tab is open.

“Console toolbar” on page 541

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.

Icon	Command name and Description
	<p>New Installation Profile</p> <p>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.</p>
	<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>
	<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 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>

Icon	Command name and Description
	<p>Run All Tasks</p> <p>Click this icon to run all the enabled tasks for the current profile.</p>

## Task toolbar


The Configuration Manager task toolbar is located at the upper right of the Task Editor pane when a Task tab is open.





The task toolbar contains the following icons for working with the current task:

Icon or Button	Command Name and Description
	<p>Enable the Selected Task</p> <p>Click this icon to enable a task. The Run All Tasks command only runs tasks that are enabled.</p>
	<p>Disable the Selected Task</p> <p>Click this icon to disable a task. The Run All Tasks command only runs tasks that are enabled.</p>
	<p>Save</p> <p>Click this icon to save the current task.</p>
<b>Test Database Connection</b>	<p>Test Database Connection</p> <p>Configure GCD JDBC Data Sources task or Configure Object Store JDBC Data Sources task tab only. Click this button to test the connection to the database by using the values provided.</p>
<b>Test LDAP Connection</b>	<p>Test LDAP Connection</p> <p>Configure LDAP task tab only. Click this button to test the connection to the directory service provider by using the values provided.</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.

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>

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 43. 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 546 for detailed procedures to create a profile.
	New Upgrade Profile	Creates a profile for upgrading Content Engine. See “Creating a profile for a new installation” on page 546 for detailed procedures to create a profile.
	Open Profile	Opens an existing profile for viewing or editing. Keyboard shortcut: Ctrl+O
	Close Profile	Closes the current profile.
	Save	Saves your changes to the active task. Keyboard shortcut: Ctrl+S

Table 43. Main Menu Commands (continued)

Menu name	Command name	Description
	Save All	Saves your changes to all open tasks. Keyboard shortcut: Ctrl+Shift+S
	Save Copy of Profile As	Saves the current profile with a new name or path.
	Edit Application Server Properties	Opens the Edit Application Server Properties wizard for editing the application server values for the profile. Keyboard shortcut: Ctrl+U
	Run All	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. Keyboard shortcut: Ctrl+R
	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	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	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.

Table 44. Profile Icon Pop-Up Menu Commands

Command	Description
Edit Application Server Properties	Opens the Edit Application Server Properties wizard for the profile.
Add New Task > Configure JDBC Data Sources	Adds a New_Configure JDBC Data Sources task to the profile.
Add New Task > Configure LDAP	Adds a New_Configure LDAP task to the profile.

Table 44. Profile Icon Pop-Up Menu Commands (continued)

Command	Description
Add New Task > Configure Bootstrap	Adds a Configure Bootstrap task to the profile.
Run All	Displays a sub-menu of the tasks associated with the profile. Click the task name that you want to run.
Close Configuration Profile	Closes the configuration profile.

Table 45. Task Icon Pop-Up Menu Commands

Command	Description
Edit Selected Task	Opens the task in the task pane for editing.
Enable Selected Task	Toggles the state of the task between enabled and disabled. Any task that is disabled will not run with either the <b>Run Selected Task</b> command or the Run All Tasks command.
Disable Selected Task	<p>If the task is currently enabled, selecting the <b>Disable Selected Task</b> command prevents the task from running, changes the font for the task icon to italic, and appends "(disabled)" to the icon label.</p> <p>If the task is currently disabled, selecting the <b>Enable Selected Task</b> command allows the task to run, restores the original font, and removes "(disabled)" from the icon label.</p>
Copy the Selected Task	Creates a copy of the selected task. This command is available only for the Configure JDBC Data Sources and the Configure LDAP tasks.
Add New Task > Configure JDBC Data Sources	Adds a Configure JDBC Data Sources task to the profile. You can have multiple Configure JDBC Data Sources tasks in a profile.
Add New Task > Configure Login Modules	Adds a Configure Login Modules task to the profile. You can only have 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 Properties	Adds a Configure Bootstrap Properties task to the profile. You can have multiple Configure Bootstrap Properties tasks in a profile.
Add New Task > Deploy Application	Adds a Deploy Application task to the profile. You can only have 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.
Check Task Status	Displays the current status of the task.
Rename Task	Opens an edit window in which you can change the name of the label associated with the task.
Delete the 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 Engine instance” on page 546

You can use the Configuration Manager graphical user interface to configure a Content Engine instance.

“Setting the password save preference” on page 546

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 546

You must create a new configuration profile for each Content Engine application that you deploy.

“Creating a profile for an upgrade” on page 547

You use the upgrade configuration profile to update the existing Content Engine bootstrap properties and deploy the updated EAR file. In order to create an upgrade profile, the Content Engine installation program must have detected an existing Content Engine installation.

“Opening and closing an existing profile or task” on page 547

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 548

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 548

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 550

You must run a task to apply the values that you provided.

“Adding an additional task to your profile” on page 552

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 Properties 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 553

You can delete any unneeded tasks from your profile.

“Running all tasks at the same time” on page 553

You can run all the tasks in a profile at the same time. Disabled tasks will not run.

“Running a single task” on page 554

You can run each configuration task individually. Disabled tasks will not run.

“Checking the task status” on page 554

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 555

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 555  
You can save your profile and task settings at any time.

## Configuring a Content Engine instance

You can use the Configuration Manager graphical user interface to configure a Content Engine instance.

To configure a Content Engine instance:

1. Create a configuration profile. See “Creating a profile for a new installation.”
2. Edit the configuration tasks included in the profile. See one or more of the following topics:
  - “Editing the configure JDBC data source task” on page 549
  - “Editing the configure LDAP task” on page 549
  - “Configuring the login modules” on page 551
  - “Editing the configure bootstrap properties settings” on page 550
3. Apply the configuration settings by running the tasks. See “Running all tasks at the same time” on page 553.
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 550.

## 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, you must specify any passwords required by the tasks and for the application server properties before you run the tasks; otherwise, the tasks won't 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 <b>Save all passwords to file when saving a task or profile</b> check box.
To prevent writing passwords to file	Clear the <b>Save all passwords to file when saving a task or profile</b> check box.

3. Click **OK**.

## Creating a profile for a new installation

You must create a new configuration profile for each Content Engine application that you deploy.

To create a new configuration profile:

1. Start the Create New Installation Profile wizard.
  - Click the **New Installation Profile** 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 Configuration 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 property description.

The new profile is displayed as an icon in the left-hand pane with icons for the tasks 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 Properties
- Deploy Application (Disabled)

### Creating a profile for an upgrade

You use the upgrade configuration profile to update the existing Content Engine bootstrap properties and deploy the updated EAR file. In order to create an upgrade profile, the Content Engine installation program must have detected an existing Content Engine installation.

1. Start the Create a Profile Wizard by using one of these methods:
  - Click **Create a Profile for an Upgrade Installation** in the toolbar.
  - Select **File** → **New 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-hand pane with the name that was presented in the confirmation screen with icons for the **Configure Bootstrap** task and the **Deploy Application** task.

### 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.

1. Open a profile:
  - Click **Open an Existing Profile** 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 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 Engine Task View pane, and then click **Edit Selected Task** in the Profile toolbar.
    - Double-click the *task name* in the Content 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.

1. Start the Edit Application Server Properties wizard by using one of these methods:
  - Click **Edit Application Server Properties** in the main 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. 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 source task” on page 549

The JDBC data source information is used by Content Engine to connect to

Global Configuration Data and 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 LDAP task”

The LDAP information is used to connect Content Engine to the directory service provider to authenticate users.

“Editing the configure bootstrap properties settings” on page 550

The bootstrap information is needed for creating the Global Configuration Data and for starting Content Engine.

“Editing the deploy application task” on page 550

You can edit the deployment property values without applying the settings.

When you apply the settings, the Content 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 Process Engine client files, Content Search Engine, or customized applications for Content Engine.

### Editing the configure JDBC data source task:

The JDBC data source information is used by Content Engine to connect to Global Configuration Data and 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 procedure for editing the Configure GCD JDBC Data Sources task and the Configure Object Store JDBC Data Sources task is the same. To complete the Content Engine configuration, you must configure the GCD data sources and the data sources for each object store.

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 field name 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 LDAP task:

The LDAP information is used to connect Content Engine to the directory service provider to authenticate users.

1. Double-click **Configure LDAP** in the Content 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 field name 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 properties settings:

The bootstrap information is needed for creating the Global Configuration Data and for starting Content Engine.

1. Double-click **Configure Bootstrap Properties** in the Content Engine Task View pane to open the task for editing.
2. Select a value for the **Bootstrap operation** field:

Option	Description
To provide bootstrap information for a new installation profile	Select <b>Create New</b> .
To modify an existing deployed EAR file	Select <b>Modify Existing</b> .
To upgrade an existing deployed EAR file	Select <b>Upgrade</b> .

3. Provide the bootstrap property values. For details on the fields, hover your mouse over the field name to view the property description.
4. Optional: If you selected **Modify Existing** or **Upgrade**, then click **Verify Bootstrap Information** to display the bootstrap information from the modified EAR file. You can verify the information in the modified EAR file for a new installation after you run the task.
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 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 Process Engine client files, Content Search Engine, or customized applications for Content 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 field name to view the property description..
3. Select **File** → **Save**.

#### Related tasks

“Configuring Content Engine” on page 21

You can configure and deploy all of your Content Engine instances with Configuration Manager. Configuration Manager prepares the Content Engine application for deployment on the application server. A single Content 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” on page 551

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.

“Configuring the login modules”

The login modules provide authentication information for the Content Engine application.

“Applying the LDAP settings” on page 552

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 properties settings” on page 552

The bootstrap information is needed for creating the Global Configuration Data and for starting Content Engine. Your bootstrap 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 552

Your Deploy Application task settings are stored when you save the task, but the Content 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.

1. Select the configure data sources task that you want to run.
  - Right-click **Configure GCD JDBC Data Sources** in the Content Engine Task View pane, and select **Run Task**.
  - Right-click **Configure Object Store JDBC Data Sources** in the Content 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.

### Configuring the login modules:

The login modules provide authentication information for the Content Engine application.

You do not must 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 configure the login modules:

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 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.
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.

### 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.

1. Right-click **Configure LDAP** in the Content 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 properties settings:

The bootstrap information is needed for creating the Global Configuration Data and for starting Content Engine. Your bootstrap settings are stored when you save the task, but the settings are not applied to the application server until you run the task.

1. Right-click **Configure Bootstrap Properties** in the Content Engine Task View pane, and then select **Run Task**. Running the configuration task can take a few minutes.
2. Optional: If you selected **Create New**, then click **Verify Bootstrap Information** to display the bootstrap information from the modified EAR file.
3. Close the Configure Bootstrap properties 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 Engine EAR file is not deployed to the application server until you run the task.

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 properties task pane.

The task execution status messages are displayed in the Console pane below the Deploy Application task properties.

### Adding an additional task to your 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 Properties 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 LDAP



- Configure Bootstrap Properties
- 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 new 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 Properties 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 LDAP
- Configure Bootstrap Properties
- Deploy Application

When you delete a task, all the property values are removed. If you later need the task, you will have to add a new task and re-enter all your values.

To delete a task from your 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 will not run.

To run all tasks in a profile:

1. If the profile is collapsed in the Content 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 Engine Task View pane toolbar.
- Select **File** → **Run All**.

**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 535.

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 Engine Task View pane, click + next to the profile name to expand it.
2. Use one of the following methods to run the Run a Task command:
  - Click the down arrow just to the right of the **Run All Tasks** icon in the Main toolbar, and then select the task that you want to run.
  - Click the *task name* in the Content Engine Task View pane to select the task. Click **Run a Task** in the Profile toolbar.
  - Right-click the *task name* in the Content 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 535.

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.

1. If the profile is collapsed in the Content Engine Task View pane, click + next to the profile name to expand it.
2. Use one of the following methods to run the Check Status command:
  - Click the *task name* in the Content Engine Task View pane, and then click **Check Status** in the Content Engine Task View pane toolbar.
  - Right-click the *task name* in the Content 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.

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.

## 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.

1. Run at least one task.
2. Use one of the following methods to run the View Log command:
  - Click **View Configuration Manager Log File** in the Main toolbar.
  - Select **Window** → **View Log**.

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.

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.

### Windows example

```
-vm
C:\Program Files\IBM\FileNet\ContentEngine\cejvm\bin
```

### UNIX example

```
-vm
/opt/IBM/FileNet/ContentEngine/_cejvm/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”

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:

Operating System	File Name
UNIX	<i>ce_install_path</i> /tools/configure/ configmgr_cl
Windows	<i>ce_install_path</i> \tools\configure\ configmgr_cl.exe

“How to read the syntax diagrams” on page 557

Syntax diagrams describe how you must enter commands and what options are available.

“**checkstatus** command” on page 557

The **checkstatus** command checks the status of the specified configuration task. The command name is not case sensitive.

“**execute** command” on page 561

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 566

The **generateconfig** command generates the configuration XML file for the specified configuration task. The command name is not case sensitive.

“**generateupgrade** command (with Servers.xml file)” on page 572

The **generateupgrade** command generates the configuration XML files for upgrading an existing Content Engine. The **generateupgrade** command has two syntax formats, depending on whether you have a valid copy of the Servers.xml file in the directory where Content Engine is installed. The command name is not case sensitive.

“**generateupgrade** command (without Servers.xml file)” on page 573

The **generateupgrade** command generates the configuration XML files for upgrading an existing Content Engine. The **generateupgrade** command has two syntax formats, depending on whether you have a valid copy of the Servers.xml file in the directory where Content Engine is installed. The command name is not case sensitive.

“**gui** command” on page 575

The **gui** command opens the Configuration Manager graphical user interface. The command is not case sensitive.

“**listservers** command” on page 575

The **listservers** command displays a list of the currently deployed Content Engine servers. Only servers that are included in the *ce\_install\_path*\Servers.xml file are listed, where *ce\_install\_path* is the location where Content Engine is installed. You must supply the server names when you create an upgrade profile with the **generateUpgrade** command.

“**listtasks** command” on page 575

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 579

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 582

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 585

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 Engine settings affected by the task.

Table 46. *task\_type* values

Option	Configuration file	Description
omitted	configurebootstrap.xml configurebootstrap. <i>n</i> .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 configurebootstrap. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Checks status for applying the settings for the Content Engine bootstrap on the application server. The bootstrap information is needed for creating the Global Configuration Data and for starting Content Engine  When you generate a second bootstrap configuration file, it is named <code>configurebootstrap.2.xml</code> . 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. For example, you might must check the status for the initial bootstrap task for the new profile and to check the status for modifying the EAR file to apply a fix pack.  If your profile contains more than one <code>configurebootstrap</code> task, then you must specify the <code>-taskfile <i>task_file_name</i></code> parameter to identify the task to check.
configurejdbcgcd	configurejdbcgcd.xml	Checks the status for configuring the JDBC connections to the Global Configuration Data (GCD) database used by Content Engine.

Table 46. *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 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 <b>-taskfile</b> <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 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 <b>-taskfile</b> <i>task_file_name</i> parameter to identify the task to check.</p>



Table 46. *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 Engine application.
deployapplication	deployapplication.xml	Checks status for deploying the Content 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 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 configurejdbcos -profile wstdb2jdbc
```

### Check the status of a profile with several files for the configurejdbcos task.

The following command checks the status of the configurejdbcos.2.xml task file in the *ce\_install\_path/tools/configure/profiles/wstdb2jdbc* directory:

```
configmgr_cl checkstatus -taskfile configurejdbcos.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 Engine settings affected by the task.

Table 47. *task\_name* values

Option	Configuration file to execute	Description
omitted	configurebootstrap.xml	If you omit the <b>-task</b> <i>task_type</i> parameter and the <b>-taskfile</b> <i>task_file_name</i> parameter, then all the configuration files in the path are run. Any configuration XML file that has the <b>enabled</b> attribute value in the <b>&lt;configuration&gt;</b> tag set to false is skipped.
	configurebootstrap. <i>n</i> .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	

Table 47. *task\_name* values (continued)

Option	Configuration file to execute	Description
configurebootstrap	configurebootstrap.xml  configurebootstrap. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	<p>Applies the settings for the Content Engine bootstrap on the application server. The bootstrap information is needed for creating the Global Configuration Data and for starting Content Engine</p> <p>When you generate a second bootstrap configuration file, it is named configurebootstrap.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. For example, you might must run the initial bootstrap task for the new profile and then later run another task for modifying the EAR file to apply a fix pack.</p> <p>If your profile contains more than one configurebootstrap task, then you must specify the <b>-taskfile</b> <i>task_file_name</i> parameter to identify the task to run.</p>
configurejdbcgcd	configurejdbcgcd.xml	Applies the settings for configuring the JDBC connections to the Global Configuration Data (GCD) database used by Content Engine.

Table 47. *task\_name* values (continued)

Option	Configuration file to execute	Description
configurejdbcos	configurejdbcos.xml  configurejdbcos. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	<p>Applies the settings for configuring JDBC connections to a single object store database used by Content 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 can edit the file name as needed.</p> <p>If your profile contains more than one configurejdbcos task, then you must specify the <b>-taskfile</b> <i>task_file_name</i> parameter to identify the task to run.</p>

Table 47. *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 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.  JBoss does not support multiple LDAP tasks.  If your profile contains more than one configureldap task, then you must specify the <b>-taskfile</b> <i>task_file_name</i> parameter to identify the task to run.  Oracle WebLogic Server only. When you run configureldap option, the weblogic.security.providers.authentication.DefaultAuthenticator.ControlFlag  value is set to SUFFICIENT for authenticating users.
configureloginmodules	configureloginmodules.xml	(WebSphere Application Server or JBoss Application Server only.) Creates the login modules for the Content Engine application.
deployapplication	deployapplication.xml	Deploys the Content Engine application on the application server.
registerem	registerem.xml	Windows only. Registers or unregistersEnterprise Manager from the Windows Registry.

**-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 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 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 Engine uses for authenticating users and must be activedirectory, adam, edirectory, oid, sunjava, 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 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 Engine deployment. The value must be `standard`, `cluster`, or `netdeploy` (network deployment).

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

Specify `netdeploy` if you are deploying Content Engine to a managed WebSphere Application Server instance. That is, you are using Network Deployment to manage individual servers that are not necessarily 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 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 Engine settings affected by the task.

Table 48. *task\_type* values

Option	Configuration file to generate	Description
omitted	applicationserver.xml configurebootstrap.xml configurejdbcgcd.xml configurejdbcos.xml configureldap.xml configureloginmodules.xml deployapplication.xml	If you omit the <code>-task task_type</code> parameter and the <code>-taskfile task_file_name</code> parameter, then all the default configuration files for a profile are created.

Table 48. *task\_type* values (continued)

Option	Configuration file to generate	Description
configurebootstrap	<p>applicationserver.xml</p> <p>configurebootstrap.xml</p> <p>configurebootstrap.<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 the Content Engine bootstrap on the application server. The bootstrap information is needed for creating the Global Configuration Data and for starting Content Engine</p> <p>When you generate a second bootstrap configuration file, it is named <code>configurebootstrap.2.xml</code>. 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. For example, you might must generate the initial bootstrap task for the new profile and then generate a second bootstrap task for modifying the EAR file to apply a fix pack.</p> <p>If the profile already contains an <code>applicationserver.xml</code> file, the existing file is retained.</p>
configurejdbcgcd	<p>applicationserver.xml</p> <p>configurejdbcgcd.xml</p>	<p>Generates the file for the application server properties and the file with the settings for configuring the JDBC connections to the Global Configuration Data (CGD) database used by Content Engine.</p> <p>If the profile already contains an <code>applicationserver.xml</code> file, the existing file is retained.</p>

Table 48. *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 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 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>JBoss does not support multiple LDAP tasks.</p> <p>If the profile already contains an applicationserver.xml file, the existing file is retained.</p>

Table 48. *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 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 Engine application on the application server.  If the profile already contains an applicationserver.xml file, the existing file is retained.
registerem	registerem.xml	Generates the file for registering or unregistering Enterprise Manager from the Windows Registry.

**-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 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 -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 -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
```

## generateupgrade command (with Servers.xml file)

The **generateupgrade** command generates the configuration XML files for upgrading an existing Content Engine. The **generateupgrade** command has two syntax formats, depending on whether you have a valid copy of the Servers.xml file in the directory where Content Engine is installed. The command name is not case sensitive.

## generateupgrade command syntax

Use the following syntax for the **generateupgrade** command if you have an existing Servers.XML file with valid server information in the directory where Content Engine is installed (*ce\_install\_path*).

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 generateupgrade -server server_name -deploy deploy_type
-profile myprofile [-silent] [-force] [-help]
```

## generateupgrade command parameters

### -server *server\_name*

The **-server** *server\_name* parameter indicates the server to create the upgrade profile for. Use the **listservers** command to display a list of valid *server\_name* values before you run the **generateupgrade** 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 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.

### **-help**

The **-help** parameter is optional and displays a brief message on the command syntax instead of running the command.

### **generateupgrade command examples**

#### **Generate the upgrade configuration files when Servers.xml file exists.**

The following command generates all the upgrade configuration XML files for a server named ceserver1 from an existing Content Engine for the profile UpgradeServer1 in the default profile directory:

```
configmgr_cl generateupgrade -server ceserver1 -profile UpgradeServer1
```

#### **Generate the upgrade configuration files when Servers.xml file exists, but does not have the deployment type.**

The following command generates all the upgrade configuration XML files for a server named ceserver1 from an existing Content Engine for the profile UpgradeServer1 in the default profile directory:

```
configmgr_cl generateupgrade -server ceserver1 -deploy cluster
-profile UpgradeServer1
```

#### **Display the help for the generateupgrade command.**

The following command displays the help for the **generateupgrade** command:

```
configmgr_cl generateupgrade -help
```

### **generateupgrade command (without Servers.xml file)**

The **generateupgrade** command generates the configuration XML files for upgrading an existing Content Engine. The **generateupgrade** command has two syntax formats, depending on whether you have a valid copy of the Servers.xml file in the directory where Content Engine is installed. The command name is not case sensitive.

### **generateupgrade command syntax**

Use the following syntax for the **generateupgrade** command if you do not have an existing Servers.XML file with valid server information in the directory where Content Engine is installed (*ce\_install\_path*).

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 generateupgrade -appserver app_server_type -server server_name
-deploy deploy_type -profile myprofile [-silent]
[-force] [-help]
```

### **generateupgrade command parameters**

#### **-appserver *appserver\_type***

The **-appserver *appserver\_type*** parameter is required only if the *ce\_install\_path/Servers.xml* file does not exist or does not contain any servers. This parameter specifies the type of application server and must be one of the following values: WebSphere, WebLogic, or JBoss.

#### **-server *server\_name***

The **-server *server\_name*** parameter indicates the server to create the upgrade profile for. Use the `listservers` command to display a list of valid *server\_name* values before you run the `generateupgrade` command.

#### **-deploy *deploy\_type***

The **-deploy *deploy\_type*** parameter is required only if the *ce\_install\_path/*



Servers.xml file does not exist or does not contain the deployment type for the selected server. This parameter specifies the type of Content Engine deployment. If a value for the deployment type exists in the Servers.xml file for the selected server, then the value from the Servers.xml file is used instead the value you specify on the command line.

Valid values are standard, cluster, or netdeploy (network deployment).

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

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

#### **-help**

The **-help** parameter is optional and displays a brief message on the command syntax instead of running the command.

### **generateupgrade command examples**

**Generate the upgrade configuration files when Servers.xml file does not exist.**

The following command generates the upgrade configuration XML files for

a server named ceserver1 from an existing Content Engine cluster deployment that uses the profile UpgradeServer1 in the default profile directory:

```
configmgr_cl generateupgrade -deploy cluster -profile UpgradeServer1
```

#### **Display the help for the generateupgrade command.**

The following command displays the help for the **generateupgrade** command:

```
configmgr_cl generateupgrade -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
```

#### **listservers command**

The **listservers** command displays a list of the currently deployed Content Engine servers. Only servers that are included in the *ce\_install\_path*\Servers.xml file are listed, where *ce\_install\_path* is the location where Content Engine is installed. You must supply the server names when you create an upgrade profile with the **generateUpgrade** command.

#### **listservers command syntax**

```
configmgr_cl listservers [-help]
```

#### **listservers command examples**

##### **List the deployed Content Engine servers.**

The following command lists the deployed Content Engine servers.

```
configmgr_cl listservers
```

A message like the following message is displayed:

These are the currently deployed Content Engine servers:

```
ce_server01Node01Cell01
 Application Server: WebSphere
 Ear file: C:\Program Files\IBM\FileNet\ContentEngine\lib\deployed\
Engine-ws.ear
 No profile is set. Use the generateUpgrade command to generate a
profile to upgrade this server.
 Deployment Type: Network
```

##### **Display the help for the listservers command.**

The following command displays the help for the **listservers** command:

```
configmgr_cl listservers -help
```

#### **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 Engine settings affected by the task.

Table 49. *task\_type* values

Option	Configuration files	Description
omitted	configurebootstrap.xml configurebootstrap. <i>n</i> .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 <b>-task</b> <i>task_type</i> parameter, then all the configuration tasks and the associated task files for the profile are listed.
configurebootstrap	configurebootstrap.xml configurebootstrap. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Lists the task for configuring the settings for the Content Engine bootstrap on the application server. The bootstrap information is needed for creating the Global Configuration Data and for starting Content Engine  When you generate a second bootstrap configuration file, it is named <code>configurebootstrap.2.xml</code> . The filename increments for each new file you generate.
configurejdbcgcd	configurejdbcgcd.xml	Lists the task for configuring the settings for the JDBC connections to the Global Configuration Data (CGD) database used by Content Engine.

Table 49. *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	Lists the task for configuring the settings for the JDBC connections to a single object store database used by Content 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 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.  JBoss Application Server does not support multiple LDAP tasks.
configureloginmodules	configureloginmodules.xml	(WebSphere Application Server or JBoss Application Server only.) Lists the task for configuring the login modules for the Content Engine application.
deployapplication	deployapplication.xml	Lists the task for deploying the Content 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 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 Properties
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 Engine settings affected by the task.

Table 50. *task\_type* values

Option	Configuration files	Description
configurebootstrap	configurebootstrap.xml  configurebootstrap. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Moves the task for configuring the settings for the Content Engine bootstrap on the application server. The bootstrap information is needed for creating the Global Configuration Data and for starting Content Engine  When you generate a second bootstrap configuration file, it is named configurebootstrap.2.xml. The filename increments for each new file you generate.

Table 50. *task\_type* values (continued)

Option	Configuration files	Description
configurejdbcgcd	configurejdbcgcd.xml	Moves the task for configuring the settings for the JDBC connections to the Global Configuration Data (CGD) database used by Content Engine.
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 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 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.  JBoss Application Server does not support multiple LDAP tasks.
configureloginmodules	configureloginmodules.xml	Moves the task for configuring the login modules for the Content Engine application.
deployapplication	deployapplication.xml	Moves the task for deploying the Content 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 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 Engine settings affected by the task.

Table 51. *task\_type* values

Option	Configuration file to remove	Description
configurebootstrap	configurebootstrap.xml  configurebootstrap. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Settings for the Content Engine bootstrap on the application server. The bootstrap information is needed for creating the Global Configuration Data and for starting Content Engine  When you generate a second bootstrap configuration file, it is named configurebootstrap.2.xml. The filename increments for each new file you generate.
configurejdbcgcd	configurejdbcgcd.xml	Settings for configuring the JDBC connections to the Global Configuration Data (CGD) database used by Content Engine.

Table 51. *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 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 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 <b>-taskfile</b> <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 Engine application.
deployapplication	deployapplication.xml	Deploys the Content 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 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.

```
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 Engine settings affected by the task.

Table 52. *task\_type* values

Option	Configuration file	Description
omitted	applicationserver.xml configurebootstrap.xml configurebootstrap. <i>n</i> .xml configurejdbcgcd.xml configurejdbcos.xml configurejdbcos. <i>n</i> .xml configureldap.xml configureldap. <i>n</i> .xml deployapplication.xml	If you omit the <b>-task</b> <i>task_type</i> parameter and the <b>-taskfile</b> <i>task_file_name</i> 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.
	Where <i>n</i> is an integer starting with 2	

Table 52. *task\_type* values (continued)

Option	Configuration file	Description
configurebootstrap	configurebootstrap.xml  configurebootstrap. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Encrypts the password for the BootstrapPassword property that is used to create the Global Configuration Data and to start Content Engine.  If you have more than one configurebootstrap. <i>n</i> .xml file, run the command for each task file.
configurejdbcgcd	configurejdbcgcd.xml	Encrypts the password for the DatabasePassword property that Content 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 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.
configureldap	configureldap.xml  configureldap. <i>n</i> .xml, where <i>n</i> is an integer starting with 2	Encrypts the password for the LDAPBindPassword property that Content Engine uses to connect to the directory server for authenticating Content Engine users.  (WebSphere Application Server or Oracle WebLogic Server only.) If you have more than one configureldap. <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 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 installation and upgrade

This section provides troubleshooting solutions for problems you might encounter when installing or upgrading IBM FileNet P8 software.

“AddOn installation can fail with resource unavailable exception”

An AddOn installation might fail if a prepared statement in the prepared server cache of an application server references the specified database table.

“Application server does not start after installation and shutdown” on page 590  
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.

“Cannot save Process Task Manager security settings” on page 591

Saving the initial Process Task Manager security settings could fail because the software or database is not running, the connection with Content Engine failed, or user credential information is not correct.

---

### AddOn installation can fail with resource unavailable exception

An AddOn installation might fail if a prepared statement in the prepared server cache of an application server references the specified database table.

#### Symptoms

The installation of an AddOn into an object store that uses a DB2 for z/OS database fails. The installation returns an exception message that indicates the database table is currently referenced by a prepared statement and cannot be altered.

#### Causes

Installing an AddOn into an object store that uses DB2 for z/OS might fail when a prepared statement that is stored in the prepared statement cache of the application server references the affected database table. This reference maintains an active association to the referenced table and thus prevents any schema modifications from occurring.

For example, a -904 resource exception message with the reason code of SQLERRMC=00E70081 indicates the table associated with the ALTER TABLE statement (DocVersion) is currently referenced by a prepared statement that is stored in the prepared statement cache and therefore, it cannot be altered.

```
2008-10-08T06:25:07.204Z 291E291E API FNRCE0230E - ERROR An error occurred
accessing the database. ErrorCode: -904, Message: 'DB2 SQL Error: SQLCODE=-904,
SQLSTATE=57011,SQLERRMC=00E70081;00000A00;A12BASE.DOCVERSION, DRIVER=3.51.118'
SQL: vargraphic(1200) "\ncom.filenet.api.exception.EngineRuntimeException:
DB_ERROR: An error occurred accessing the database.
ErrorCode: -904, Message: 'DB2 SQL Error: SQLCODE=-904, SQLSTATE=57011,
SQLERRMC=00E70081;00000A00;A12BASE.DOCVERSION, DRIVER=3.51.118'
SQL: "ALTER TABLE DocVersion ADD COLUMN uee8_rmentitydescription vargraphic(1200)"
```

#### Resolving the problem

Disable the prepared statement cache for the XA data source of the affected object store. Additionally, ensure the DB2 for z/OS **CACHEDYN** subsystem parameter is set to YES.

To disable the prepared statement cache for the XA data source of the object store:

1. Go to the prepared statement cache for the XA data source of the affected object store.
2. Make a note of this current statement size value to use when you reset it.
3. Disable the prepared statement cache for the XA data source of the affected object store by setting the statement size to 0.
4. Set the DB2 for z/OS **CACHEDYN** subsystem parameter to YES if needed.
5. Run the AddOn installation.
6. In the prepared statement cache for the XA data source of the affected object store, reset the statement size to its previous value.

---

## Application server does not start after installation and shutdown

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.

---

## Cannot save Process Task Manager security settings

Saving the initial Process Task Manager security settings could fail because the software or database is not running, the connection with Content Engine failed, or user credential information is not correct.

To save Process Task Manager security settings, the following conditions must be true:

- Process Engine software and the database must be running.
- Process Engine must be able to connect to the Content Engine by using the URI configured in Process Task Manager.
- All user names, groups, and passwords must match the names that are configured in the Content Engine LDAP configuration.

After all connections are made and security information is verified, the configuration is written to the Process Engine database. If the security settings cannot be saved, start by checking the following log files.

Operating system	Log file location
UNIX	<code>/fnsw/local/logs/TM_daemon/ PEDirectoryServerConnectionDebug.txt</code>
Windows	<code>\fnsw_loc\logs\TM_daemon\ PEDirectoryServerConnectionDebug.txt</code>

After you review the log files, the following procedures provide information to assist with identifying the source of the problem.

“Verifying the Content Engine server is available to Process Engine on the network” on page 592

To save Process Engine security settings from Process Task Manager, the server where Content Engine is installed must be available to Process Engine on the network.

“Verifying that the Process Engine can connect to a FileNet Engine Web page on Content Engine” on page 592

Verify that Process Engine can connect to the FileNet Engine Web page on Content Engine. Failures could indicate an incorrect server name or problems with the designated port.

“Verifying that Process Engine can connect to Content Engine by using the Content Engine URI” on page 593

Verify that Process Engine can connect to the Content Engine by using the Content Engine URI. Failures could indicate problems connecting to the Content Engine or problems with security settings.

## Verifying the Content Engine server is available to Process Engine on the network

To save Process Engine security settings from Process Task Manager, the server where Content Engine is installed must be available to Process Engine on the network.

To ping the server and verify that the Process Engine server can connect to the Content Engine server on the network:

1. Open a Web browser on the Process Engine server.
2. Ping the server by running the following command: `ping ceserver`

You should see responses that are similar to these:

```
Pinging ceserver [1.2.3.4]
Reply from 1.2.3.4: bytes =32 time < 1ms TTL=127
Reply from 1.2.3.4: bytes =32 time < 1ms TTL=127
Reply from 1.2.3.4: bytes =32 time < 1ms TTL=127
Reply from 1.2.3.4: bytes =32 time < 1ms TTL=127
```

The format varies, but the messages indicate there was a reply from the server and the IP address of this server is 1.2.3.4. If the ping returns a message indicating the host could not be found, verify that the server is running, the server name is correct, there is no DNS or firewall issue, and try again.

## Verifying that the Process Engine can connect to a FileNet Engine Web page on Content Engine

Verify that Process Engine can connect to the FileNet Engine Web page on Content Engine. Failures could indicate an incorrect server name or problems with the designated port.

To verify that the Process Engine server can access the FileNet Engine Web page on the Content Engine and verify that the software version on the Content Engine matches the version of Content Engine Client software installed on the Process Engine:

1. Open a Web browser on the Process Engine server.
2. Browse to the FileNet Engine Web page and enter: `http://ceserver:port/FileNet/Engine`

*ceserver*

The host name of the machine where Content Engine is deployed.

*port*

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

The following table describes an example address for your application server.

Application server type	Web page address
IBM WebSphere Application Server	<code>http://myserver:9080/FileNet/Engine</code>
Oracle WebLogic Server	<code>http://myserver:7001/FileNet/Engine</code>
JBoss Application Server	<code>http://myserver:8080/FileNet/Engine</code>

3. Verify the value in the **Startup Message** key. The Content Engine build and version (for example, dap451.100), must match the build and version in the `version.txt` file in the TAR or ZIP file of the Content Engine Client installation software on Process Engine.

If you are able to retrieve the FileNet Engine information, the Content Engine server is available and configured correctly.

If you are able to retrieve the information but the Content Engine and Content Engine Client software versions are not the same, you must install the correct version of the Content Engine Client software.

If you are not able to retrieve the information, verify that the server can be reached by pinging the Content Engine server (*ceserver*).

If you can ping the server with the *ceserver* name, the problem could be with the port number that you are trying to use. Or the server that you can ping is not a Content Engine server, even though it responds on the network.

## Verifying that Process Engine can connect to Content Engine by using the Content Engine URI

Verify that Process Engine can connect to the Content Engine by using the Content Engine URI. Failures could indicate problems connecting to the Content Engine or problems with security settings.

To verify that the Process Engine server can connect to the Content Engine by using the Content Engine URI and the security information specified in Process Task Manager:

1. Open a Web browser on the Process Engine server. Enter the Content Engine URI that is configured in Process Task Manager. In these examples, the protocol is HTTP and the attachment protocol is MTOM. The attachment protocol can also be specified as FNCEWS40DIME.

Application server type	Web page address
IBM WebSphere Application Server	<a href="http://CEServer:9080/wsi/FNCEWS40MTOM/">http://CEServer:9080/wsi/FNCEWS40MTOM/</a>
Oracle WebLogic Server	<a href="http://CEServer:7001/wsi/FNCEWS40MTOM/">http://CEServer:7001/wsi/FNCEWS40MTOM/</a>
JBoss Application Server	<a href="http://CEServer:8080/wsi/FNCEWS40MTOM/">http://CEServer:8080/wsi/FNCEWS40MTOM/</a>

2. If you can connect to the Content Engine by using the URI, try to save the security settings by clicking **Apply**. If an error is returned, you verified the ability to connect to Content Engine, so security information might not be correct, including the user name, password, or group names. Check the following log files for specific information related to problems with the security settings.

Operating system	Log file location
UNIX	/fnsw/local/logs/TM_daemon/ PEDirectoryServerConnectionDebug.txt
Windows	\fnsw_loc\logs\TM_daemon\ PEDirectoryServerConnectionDebug.txt

The service user name must be a member of the group that is specified in the Process Engine Administrator Group (*pe\_admin\_group*). The user name must be entered as a short name. Duplicate short names are not supported.





---

## 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.  
3-2-12, Roppongi, Minato-ku, Tokyo 106-8711 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](http://www.ibm.com/legal/copytrade.shtml)).

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

- add-on component upgrade 487
- additional file storage areas 181
- AddOn installation problems
  - troubleshooting 589
- Administration servers
  - configuring 299
- Application Engine
  - access roles 160
  - administrator access roles 160
  - administrators 160
  - Application Name 162
  - configuring for upgrades from 3.5 457
  - configuring on all application servers 131
  - configuring on JBoss 150
  - configuring on JBoss upgrade 475
  - configuring on WebLogic 144, 148
  - configuring on WebLogic 9.2 475
  - configuring on WebLogic
    - upgrade 470, 474
  - configuring on WebSphere 132
  - configuring SSL 171
  - configuring SSO 461, 470
  - configuring upgrades on WebSphere 458
  - container-managed authentication 458
  - container-managed authentication on WebSphere 132
  - copying custom data for upgrade 478
  - deploying on all application servers 152
  - deploying on JBoss 158, 159, 484, 485
  - deploying on WebLogic 156, 157, 483
  - deploying on WebLogic upgrade 484
  - deploying on WebSphere 153, 478, 479
  - deploying on WebSphere 6.1 154
  - deploying on WebSphere 6.1 upgrade 480
  - deploying on WebSphere 7.0 155
  - deploying on WebSphere 7.0 upgrade 481
  - deploying upgrade 480
  - editing web.xml on WebSphere 458
  - indexing 162
  - installing 123
  - installing and configuring 123
  - installing Content Engine Client 126
  - installing interactively 124
  - installing silently 125
  - installing software updates 126
  - installing software updates upgrade 448
  - multiple instances 189
  - post-upgrade configuration 486
  - preparing for upgrade 440
  - removing ISRA servlet 523

- Application Engine (*continued*)
  - removing on JBoss 521
  - removing on WebLogic 519
  - removing on WebSphere 517
  - setting up full SSL support 172
  - upgrade introduction 439
  - upgrading 443
  - upgrading from 3.5 443
  - upgrading from 3.5 interactively 444
  - upgrading from 3.5 silently 445
  - upgrading from 4.0 446
  - upgrading from 4.0 interactively 446
  - upgrading from 4.0 silently 447
- Application Integration
  - installing 184
  - installing interactively 184
  - installing silently 185
  - upgrading 487, 488
  - verify installation 186
  - verifying upgrade 489
- automatic upgrades for Content Engine data 375
- Autonomy K2
  - installing Content Search Engine 79
  - moving administration servers 202
  - non-English locales 93
  - starting or stopping on UNIX 291
  - updating user fields 294, 389
- Autonomy K2 administration server
  - installing additional interactively UNIX 197
  - installing additional silently UNIX 198
    - Windows 201
- Autonomy K2 administration servers
  - installing additional interactively Windows 200
  - UNIX 196
  - Windows 200
- Autonomy K2 server
  - modifying configuration 195
- Autonomy K2 servers
  - moving 202
- Autonomy K2 services
  - starting and stopping 199
- Autonomy K2 services (UNIX)
  - starting and stopping 85
- auxiliary documentation 6

## B

- back up after upgrade
  - Process Engine 434, 436
- banner image
  - changing 160
- bootstrap 30, 241
- bootstrap preferences
  - configuring 159
  - enhanced time zone 163
  - setting on first login 160

- bootstrap preferences (*continued*)
  - setting the SSL configuration for Application Engine 160
- bootstrap properties 550
- bootstrap.properties file
  - sharing between Application Engines 173

## C

- CBR-enabled database properties 223
- CCL 203
- CFS-IS
  - updating the settings 302
- checking the status of a task from the command line 46, 257
- checking the task status from the command line 46, 47, 257, 258
- checkstatus command 557
- COM compatibility layer 203
- COM objects upgrade 490
- Component Manager 179
- configmgr.ini 555
- configuration and startup tasks 165
- Configuration manager
  - overview 531
- Configuration Manager
  - config\_mgr\_user* permissions 23, 349
  - adding an SSL signer to the keystore 536, 537
  - adding new tasks 552
  - applying configuration settings from the command line 42, 44, 253
  - applying the Configure Bootstrap Properties settings 552
  - applying the Configure JDBC Data Sources settings 551
  - applying the values in a task 550
  - changing password preference for installation 26
  - changing password preference for upgrade 236
  - checking the status of a task 554
  - checking the status of a task from the command line 46, 257
  - checking the task status from the command line 47, 257, 258
  - checkstatus command 557
  - command line interface 32, 242
  - command-line reference 555
  - Configure Bootstrap settings for installation 241
  - Configure Bootstrap settings for upgrade 30
  - configuring Content Engine using the graphical user interface 24, 235
  - console toolbar 541
  - creating a new profile 546
  - creating an upgrade profile 352, 547
  - deploying Content Engine 552

- Configuration Manager *(continued)*
  - editing a configuration XML file for installation 39
  - editing a configuration XML file for upgrade 250
  - editing a task 548
  - editing the application server properties 548
  - editing the Configure Bootstrap Properties task 550
  - editing the Configure JDBC Data Sources task 549
  - editing the Configure LDAP task 549
  - editing the Deploy Application task 550
  - execute command 561
  - generateconfig command 566
  - generateupgrade command 572, 573
  - generating a configuration XML file for installation 35, 37
  - generating a configuration XML file for upgrade 246, 248
  - generating all of the configuration XML files at the same time for installation 34
  - generating all of the configuration XML files at the same time for upgrade 244
  - grant user permissions 23, 349
  - graphical user interface and command-line interface differences 534
  - gui command 575
  - GUI reference 538
  - installation worksheet 534
  - listservers command 575
  - listtasks command 576
  - logs 535
  - main toolbar 540
  - menus and commands 542
  - movetask command 579
  - new profile 26
  - opening an existing profile 547
  - overview 532
  - password preference 352
  - passwords 535
  - profile concepts 532
  - profile toolbar 540
  - reference 531
  - remove task 553
  - removetask command 582
  - running configuration XML files for installation 42
  - running a selected task 554
  - running all configuration XML files at the same time 42, 253
  - running all tasks at the same time 553
  - running commands 555
  - running configuration XML files for upgrade 253
  - running configuration XML files one at a time 44, 254
  - saving changes to a task or profile 555
  - setting password save preference 546
  - starting 25

- Configuration Manager *(continued)*
  - starting for installation 538
  - starting for upgrade 235
  - starting the graphical user interface for upgrade 351
  - storepasswords command 585
  - task status 554
  - task toolbar 541
  - viewing the session log 555
  - window description 539
  - working in the Configuration Manager window 539
  - working with 545
  - configuration profile
    - adding new tasks 552
    - creating a new profile 26, 237
    - renaming tasks 552
  - configuration tasks
    - adding 552
    - renaming 552
  - configuration XML files
    - applying installation settings in Configuration Manager 42
    - applying upgrade settings in Configuration Manager 253
  - Configure Bootstrap settings 30, 241
  - Configure Global Configuration Data (GCD) data source 27, 238
  - Configure LDAP 552
  - Configure LDAP task 29, 240
  - Configure Login Modules task 28, 29, 239, 240
  - configure object store data source 73, 284
  - configuring Content Engine 22, 24, 233, 350
  - configuring Content Engine using the Configuration Manager graphical user interface 24, 235
  - configuring directory service authentication 277
  - configuring login modules for Content Engine 551
  - configuring upgraded Content Engine instances by using the command line 354
  - configuring upgraded instances by using the command line 354
  - connection point
    - configure for Application Engine 167
    - migrate process router to 432
    - see connection point 432
  - connection points
    - creating for Process Engine 166
  - container-managed authentication 458
  - Application Engine on WebSphere 132
  - Content Consistency Checker 224
  - Content Engine 354
    - authentication 277
    - automatic upgrade 375
    - beginning the upgrade from version 3.5 225
    - bootstrap settings 30, 241
    - client files 276
    - completing pre-upgrade configuration 218

- Content Engine *(continued)*
  - configuring 22, 24, 233, 350
  - configuring an instance 546
  - configuring authentication 320
  - configuring directory service authentication 277
  - configuring storage devices 279
  - configuring upgraded instances
    - graphical user interface 351
  - Content Engine\ Web Upgrade Tool 306
  - creating a profile by using the command line 33, 243
  - data source XML files 339
  - deploying in a cluster for JBoss 54
  - deploying instances 48
  - deploying instances using the GUI 49
  - deploying upgraded instances 259, 358, 360
    - command line 261
    - graphical user interface 259, 359
  - deployment data 346
  - fixed content devices 320
  - generating configuration XML files 33, 243
  - IBM FileNet Content Engine Web Upgrade Tool 306, 308
  - installing 13
  - installing and configuring 11
  - installing Client files 377
  - installing Content Search Engine Client files 228, 345, 347
  - installing EMC Centera SDK library files for upgrade 269
  - installing interactively 14, 226
  - installing Process Engine Client files 19
  - installing silently 15
  - installing software updates 16, 228, 345
  - JBoss Application Server 308
  - JDBC driver 318
  - login modules 28, 29, 239, 240, 551
  - object store parameters 320
  - Oracle WebLogic Server 308
  - overview of upgrade from version 3.5 225
  - post deployment steps 65
  - post-deployment steps 272, 372
    - JBoss 67, 273, 373
    - WebLogic 67, 273, 373
    - WebSphere 66, 273, 373
  - pre-upgrade configuration 334
  - removing 505
  - removing Content Search Engine Client files 346
  - removing data 506
  - removing interactively on UNIX 505
  - removing silently 506
  - reserved words 223, 337
  - Send eMail handler 493
  - specify for Application Engine 443, 444, 445
  - SSL signer error 536, 537
  - storage device source files 55, 262, 362



- Content Engine *(continued)*
    - trace log file 278
    - uninstalling 339
    - uninstalling interactively 340
    - uninstalling silently 340
    - updating Vital Product Data 335
    - upgrade bootstrap properties 353
    - upgrade data 303
    - upgrade profile 352
    - upgrader batch file 318
    - Upgrader tool 320
      - command line 325, 326
      - upgrade.xml 326
    - upgrading
      - version 3.5 217
      - version 4.0.1 or 4.5.0 332
    - upgrading and configuring 217
    - upgrading interactively 226
    - upgrading interactively on UNIX 343
    - upgrading interactively on Windows 342
    - upgrading silently on UNIX 344
    - upgrading silently on Windows 343
    - upgrading software 341
    - upgrading software from version 3.5.x silently 227
    - using command line interface to configure 32, 242
    - verify installation 77
    - verifying deployment 67, 274, 374
    - web application server cache 338
    - web service 168, 169
    - WebSphere 306
    - XML upgrade status file 320
  - Content Engine Client
    - installing interactively on Application Engine 127
    - installing on Application Engine 126
    - installing on Application Engine upgrade 449
    - installing silently on Application Engine 128
    - removing from Application Engine 449
    - removing from Application Engine UNIX 450
    - removing from Application Engine Windows 450
    - upgrading on Application Engine interactively 451
    - upgrading on Application Engine silently 452
  - Content Engine client files
    - upgrading 418
    - upgrading on Process Engine 416
  - Content Engine Client Updater
    - uninstalling 339
    - uninstalling interactively 341
    - uninstalling silently 341
  - Content Engine upgrade 223
    - backing up the database 224, 336
    - CFS Exporter 337
    - Content Federation Services 337
    - custom subclasses of the PublishRequest object 221
  - Content Engine upgrade *(continued)*
    - in-progress Content Engine transactions involving content files 221
    - in-progress events 220
    - permissions for Engine-DS.xml 336
    - preventing name conflict with reserved words 337
    - preventing name conflicts with reserved words 223
    - publishing requests 220, 334
    - Records Manager object stores 223
    - remove accented characters in file store path 222
    - removing the deployed FileNetEngine application 337
    - stopping and disabling services 224
    - undeploying the EAR file 337
    - verify the directory permissions 222
    - webSphereDefaultIsolationLevel custom property 335
  - Content Engine Upgrader tool 318
  - Content Engine Web Upgrade Tool 306, 310
    - JBoss Application Server 308
    - Oracle WebLogic Server 308
    - starting Content Engine Web Upgrade Tool 309
    - WebSphere 306
  - Content Federation Services 337
  - Content Search Engine 196, 200
    - adding administration servers 196
    - CBR indexing 98, 328
    - CBR locale 98
    - CBREnabled flag 98
    - class properties 98, 328
    - collections 88, 294
    - collections directory 96, 299, 300
    - completing upgrade 302
    - configuring additional administration servers 201
    - configuring CBR 81, 88
    - configuring services 92
    - enabling CBR 328
    - FileNet Styleset 88, 294
    - installing additional locales 93
      - Windows 95
    - installing and configuring 79
    - installing Client files 17
      - interactively 17, 229, 347
      - silently 18, 230, 348
    - installing interactively on UNIX 81
    - installing interactively on Windows 86
    - installing on UNIX 81
    - installing on Windows 86
    - installing silently on UNIX 83
    - installing silently on Windows 87
    - installing with Autonomy K2 79
    - K2 Administrative Users 88, 294
    - K2 Broker Server 98
    - K2 Dashboard documentation 287
    - K2 Index Server 88, 294
    - K2 Search Server 88, 294
    - K2 Ticket Server 88, 294
    - K2Dashboard documentation 80
    - launching K2 Dashboard 88, 294
  - Content Search Engine *(continued)*
    - production environment
      - upgrades 287
    - removing 507
    - removing locales on UNIX 509
    - removing locales on Windows 511
    - removing servers 203
    - setting Autonomy K2 Administration Security 88, 294
    - setting environment variables 198, 291
    - upgrading 378
    - upgrading and configuring 217
    - upgrading CBR 377
    - upgrading interactively on UNIX 289, 379
    - upgrading interactively on Windows 293, 385
    - upgrading on UNIX 288, 378
    - upgrading on Windows 292, 384
    - upgrading silently on UNIX 290, 381
    - upgrading silently on Windows 294, 386
    - verifying installation 101
  - Content-Based Retrieval
    - upgrading 286, 377
  - creating a Content Engine upgrade configuration profile 352
  - creating a new profile
    - Configuration Manager 546
  - creating an upgrade profile
    - Configuration Manager 547
- ## D
- data source 73, 284
    - Global Configuration Data (GCD) 27, 238
  - data source XML files 339
  - data sources 71, 74, 283, 285
    - creating 71, 282
    - deleting 23
  - deleting existing data sources 23
  - deploy application 550
  - deploy application task 53
  - deployapplication.xml file 51, 53
  - deploying Content Engine 50
  - deployment configuration files 52
  - Deployment Manager 183
  - document
    - check in (verify new object store) 77
    - check out (verify newobject store) 77
    - create (verify new object store) 77
  - documentation 209
    - application server requirements 4
    - auxiliary 6
    - before you install 4
    - configuring site preference settings for 160
    - custom documentation 6
    - expansion product 6
    - indexing 6
    - refreshing without uninstalling 209
    - server upgrade 209
    - server URL 129, 130
    - uninstalling to upgrade 210



- documentation (*continued*)
  - updating on IBM WebSphere Application Server 210
  - updating on Oracle WebLogic Server 211, 212
  - updating the search index 213
  - upgrading 207
  - verifying web application for 214
- domain
  - users group 76
  - Verity (K2) 98
- domain, FileNet P8
  - configure permissions 69
  - configurepermissions 278
  - create 69, 276, 277

## E

- editing a configuration XML file 39, 250
- editing a configuration XML file using the command line 250
- EJB transport 168, 169
- EMC Centera SDK 63
  - configuring environment variables 270, 370
  - installing library files 269, 368, 369
- EMC Centera SDK library files
  - installing for Content Engine upgrade 269
  - installing for use with Content Engine 62
- EMC Centera SDK version 3.2 library files
  - installing 62
- Enterprise Manager
  - enable SSL 171
  - installing 15
  - installing additional instances 180
  - upgrading 331, 344
- event logs 396
- execute command 561

## F

- file document handler 490
- file storage
  - verifying 182
- file storage area
  - specify 76
- File Tracker
  - installing 186
  - installing interactively 187
  - installing silently 188
  - upgrading 487, 489
- FileNet P8
  - disaster recovery 9
  - redeployment 9
  - removing documentation 503
  - removing documentation from JBoss 504
  - removing documentation from WebLogic 504
  - removing documentation from WebSphere 503
  - removing software 501

- FileNet P8 documentation
  - configure for Process Engine help 129
  - configuring for Process Engine help 129, 130
  - upgrade 209
    - documentation 209
  - upgrading 207
  - upgrading and configuring 205
- FileNet Styleset 88
  - Content Search Engine 294
- fsa1 directory 182

## G

- generateconfig command 566
- generateupgrade command 354, 572, 573
- generating a configuration XML file 35, 37, 246, 248
- generating all of the configuration XML files at the same time 34, 244
- generating configuration XML files 33, 243
- Global Configuration Data (GCD)
  - creating 276
- gui command 575

## H

- how to read syntax diagrams 557

## I

- IBM FileNet Content Engine Web Upgrade Tool
  - JBoss Application Server 308
  - Oracle WebLogic Server 308
  - WebSphere 306
- IBM FileNet Image Services
  - updating the CFS-IS settings 302
- IBM FileNet P8 System Health page 67, 274, 374
- IBM Tivoli Directory Server 29, 240
- IIOp protocol 168, 169
- Image Services
  - updating the CFS-IS settings 302
- Image Services Integration 486
- Image Services library documents 195
- Image Services logon through LDAP 499
- indexing documentation 6
- Install Process Engine
  - interactively on UNIX 107
  - interactively on Windows 107
  - silently on UNIX 109
  - silently on Windows 109
- installation 1
  - optional tasks 177
  - troubleshooting 589
- installing
  - Content Engine 15, 226
  - Tivoli Storage Manager 55, 60, 263, 264, 267, 362, 366
    - JBoss 366
    - WebSphere 362

- installing additional Autonomy K2 administration servers on UNIX 196
- Installing Content Engine and related client software 12
- installing Content Engine Client files silently 452
- installing Content Engine software
  - updates 228, 345
- into a new version 4.5.1 FileNet P8 domain 310
- into an existing version 4.5.1 FileNet P8 domain 313
- IP address
  - Application Engine SSL host 172
  - Content Search Engine server 80, 287
- IPv4
  - defaulting to 116
- IS library documents 499
- isolated region for Process Engine 165
- ISRA
  - component software updates 499
  - enabling support for SSL 498
  - installing the servlet 192
  - site preferences 498
  - SSL configurations 192
  - SSL support 495
- ISRA servlet
  - upgrading 496

## J

- Java Virtual Machine
  - Application Engine WebSphere upgrade 465
- Java Virtual Machine settings on Application Engine Websphere 139
- JBoss
  - configuring Application Engine 150
  - configuring Application Engine upgrade 475
  - deploying Application Engine 158, 159
  - deploying Application Engine for upgrade 484, 485
- JDBC data source
  - Global Configuration Data (GCD) 27, 238
- JDBC driver 318

## K

- K2 Administration Server
  - setting logon user 87
- K2 servers
  - enabling 100
- Kerberos 168, 169

## L

- LDAP
  - authentication for ISRA 499
  - configuring on WebLogic 148
  - federated repositories on WebSphere 143, 469
  - Image Services login 195
  - stand-alone on WebSphere 142, 468

- listservers command 575
- listtasks command 576
- locales
  - removing on UNIX 509
  - removing on Windows 511
- log event handler 491
- log files
  - Configuration Manager 535
- login modules for Content Engine 28, 29, 239, 240
- LTPA
  - configuring on Application Engine 140
  - LTPA on WebSphere 466

## M

- Microsoft Office
  - installing application integration for 184
- move fixed content device data 224
- movetask command 579
- multi-server configuration
  - Application Engine 189
  - Enterprise Manager 180

## N

- new profile 237
- non-English locales 93

## O

- object store 73, 76, 284
  - automatic upgrade 375
  - data sources 71, 74, 283, 285
  - upgrade 323
  - verify new 77
- object store data source 73, 284
- options for Windows 301

## P

- P8 documentation 3
  - installing 5
  - starting and verifying 9
- password encryption
  - Process Engine 110, 413
- password preference 546
- passwords
  - Configuration Manager 535
- post-upgrade
  - Process Engine 421
- post-upgrade scripts
  - DB2 429, 431
  - Process Engine 430, 431
  - SQL Server 429, 430
- pre-upgrade
  - Process Engine 391
- Process Analyzer
  - pre-upgrade steps 393
  - verifying published events 394
- Process Analyzer events 392
- Process Analyzer, upgrade procedure 487

- Process Engine
  - /etc/inittab file 415
  - cleaning up before starting software on UNIX 115
  - completing post-installation on Windows 116
  - completing upgrade from 3.5 421, 422
  - completing upgrade from 3.5 with DB2 423
  - completing upgrade from 3.5 with Oracle 422
  - completing upgrade from 3.5 with SQL Server 425
  - completing upgrade from 4.0 or higher 434
  - Component Integrator 178
    - configuring regions after upgrade 432, 433
  - configuring shared memory 431, 436
  - configuring shared memory on Windows 121
  - connection to Component Manager 180
  - creating connection points 166
  - editing /etc/inittab on UNIX 115, 407
  - installing 103
  - installing and configuring 103
  - installing Client files 231, 356
    - interactively 19
    - silently 20
  - installing Content Engine client files 116
  - installing Content Engine client files interactively 117
  - installing Content Engine client files silently 118
  - installing interactively 106
  - installing silently 108
  - installing software updates 122, 437
  - isolated regions 393, 398
  - modifying integrity level of executables 116
  - post-installation on UNIX 114
  - post-installation with Oracle 114
  - re-enable Oracle password complexity verification 114
  - removing on UNIX 515
  - removing on Windows 513
  - removing routers after upgrade 427
  - resetting administrative passwords 111
  - restarting software 113
  - setting f\_maint an f\_sw passwords 406
  - setting f\_maint an f\_sw passwords on DB2 113, 406
  - setting f\_maint an f\_sw passwords on Oracle and SQL Server 406, 414
  - setting f\_maint and f\_sw passwords on Oracle and SQL Server 112
  - setting passwords 414
  - stopping all services and applications 396, 397, 399, 400
  - uninstalling Content Engine client files 416, 417

- Process Engine (*continued*)
  - updating email notification after upgrade 433
  - updating security 427
  - upgrading 391, 400
  - upgrading Content Engine client files 416
  - upgrading Content Engine client files interactively 418
  - upgrading Content Engine client files silently 419
  - upgrading interactively 231, 357, 404
  - upgrading silently 232, 357, 411
  - upgrading silently on Windows 411
  - verifying database connection 121, 401, 408
    - DB2 409
    - Oracle 410
    - SQL 409
  - verifying database connection after installation 113
  - verifying DB2 database connection 106, 402
  - verifying Oracle database connection 104, 403
  - verifying SQL Server database connection 105, 402
  - verifying transmitted events 394
- Process Engine Client
  - installing on Content Engine 19
  - upgrading interactively on Application Engine 455
  - upgrading on Application Engine 455
  - upgrading silently on Application Engine 456
- Process Engine client files
  - installing 437
- Process Engine I
  - verifying database connection 104
- process router
  - see connection point 432
- Process Task Manager
  - configuring 119
  - configuring for dual stack 119
  - configuring security 119
  - creating isolated regions 119
- production environments
  - upgrading 377
- profile 532
- publishing capabilities 178
- publishing components
  - upgrading 489

## R

- realm
  - configuring more than one 174
  - object store administrator 76
- refreshing 209
- remove task 553
- removetask command 582
- Rendition Engine 178
- requirements for hardware and software 207
- restore custom modifications 415
  - Process Engine 407

restore custom modifications (*continued*)  
restoring custom modifications on  
UNIX 114

## S

saving passwords to file in Configuration  
Manager 26, 236, 352  
security  
setting up SSL for Application  
Engine 171  
SSL for Content Engine 169  
SSL preference setting for Application  
Engine 160  
SSL, set up for Content Engine 168  
updating for Process Engine 427  
server-side script upgrade 490  
silent install  
Process Engine(AIX) 412  
Site preference settings  
documentation URL 160  
name and location 160  
site preferences  
configuring for ISRA 498  
ISRA 194  
single index for Application  
Name 162  
SnapLock 280  
SSL  
adding an SSL signer to the  
keystore 536  
correcting SSL Signer Exchange  
Prompt errors 537  
full support on Application  
Engine 172  
Java applets 174  
security info preference 160  
set up for Content Engine 169  
setting up for Application  
Engine 171  
setting up for Content Engine 168  
SSO 457  
configuring for Application Engine on  
WebLogic 145  
configuring for Application Engine on  
WebSphere 135  
editing configuration files 461, 470  
Starting Configuration Manager 235, 351  
Statement Cache Size 69  
statistics records 396  
storage device source files 55, 262, 362  
storepasswords command 585  
subfolder, create, (verify new object  
store) 77  
syntax diagrams 557  
System Manager 195

## T

T3 protocol 168  
T3protocol 169  
Tivoli Storage Manager  
adding native API library paths  
JBoss 59, 267, 366  
WebLogic 264, 363  
WebSphere 55, 263, 362

Tivoli Storage Manager (*continued*)

copying API libraries  
JBoss 60  
copying API libraries  
JBoss 267, 367  
WebLogic 264, 364  
WebSphere 263, 363  
copying API libraries to additional  
servers 56  
copying API library files 57  
creating a shared library  
definition 57  
installing  
JBoss 59, 60, 267, 366  
WebLogic 264, 363  
WebSphere 55, 263, 362, 366  
installing client software 55, 263, 264  
JBoss 267  
shared library definitions 367  
JBoss 60, 267  
WebLogic 265, 364  
WebSphere 56, 263, 363  
Tivoli Storage Manager client  
installing 57  
installing and adding API library  
paths 56  
troubleshooting  
AddOn installation failure 589  
application server does not start 590  
application server problems  
troubleshooting 590  
connecting to the FileNet Engine Web  
page on the Content Engine 592  
installation 589  
ping the Content Engine server 592  
Process Engine  
cannot save security settings 591  
Process Task Manager 591  
verify the Content Engine server  
responds on the network 592  
Process Engine connect to Content  
Engine using the URI 593  
upgrade 589

## U

Updating the database storage area  
parameters 328  
upgrade  
Application Integration 487  
Content Engine data 303  
ISRA Servlet 494  
move fixed content device data 224  
publishing components 489  
run the Content Consistency  
Checker 224  
troubleshooting 589  
upgrade Content Engine 353  
upgrade Content Engine bootstrap  
properties 353  
upgrade methods 209  
Upgrade Process Engine  
interactively 401  
interactively on UNIX 405  
interactively on Windows 404  
silently 408

upgrade profile  
Configuration Manager 547  
upgrader batch file 318  
Upgrader tool  
Content Engine 320  
upgrading  
Content Engine 226  
Content Search Engine 286  
Content Search Engine interactively  
on UNIX 289, 379  
Content Search Engine interactively  
on Windows 293  
Content Search Engine silently on  
UNIX 290, 381  
Content Search Engine silently on  
Windows 294  
Content-Based Retrieval 286, 377  
production environments 377  
Upgrading a version 3.5.2 FileNet P8  
domain 310, 313  
upgrading Content Engine  
preventing name conflicts with  
reserved words 223  
Upgrading Content Engine  
accented characters in file store  
path 222  
backing up the database 224, 336  
CFS Exporter 337  
Content Federation Services 337  
custom subclasses of the  
PublishRequest object 221  
in-progress Content Engine  
transactions involving content  
files 221  
in-progress events 220  
permissions for Engine-DS.xml 336  
preventing name conflict with  
reserved words 337  
publishing requests 220, 334  
Records Manager object stores 223  
removing the deployed FileNetEngine  
application 337  
stopping and disabling services 224  
undeploying the EAR file 337  
verify the directory permissions 222  
webSphereDefaultIsolationLevel  
custom property 335  
Upgrading Content Engine data  
using Content Engine Upgrader  
tool 317  
using Content Engine Web Upgrade  
Tool 305  
validating object stores 316  
upgrading Content Engine software from  
version 3.5.2 silently 227  
upgrading Enterprise Manager 331, 344  
upgrading file plan object stores 223  
Upgrading object stores 314  
Updating the database storage area  
parameters 328  
upgrading on UNIX  
Content Search Engine 378  
upgrading on Windows  
Content Search Engine 384  
upgrading Records Manager object  
stores 223

- User credentials for Application Engine
  - on WebLogic 149
- User Token
  - configuring 160
- UTCryptoKeyfile.properties 123

## V

- Validating object stores 310
- verifying Content Engine
  - deployment 67, 274, 374
- Verity Domain Config. tab (VDC) 98
- vwlog 399
- vwverify 392, 397

## W

- WAR or EAR file
  - re-creating on JBoss 158, 484
  - re-creating on WebLogic 156, 483
  - re-creating on WebSphere 153, 479
- web application server cache 338
- web services
  - Content Engine 168, 169
  - Process Engine 168, 169
- web.xml
  - editing for Application Engine SSO on WebLogic 145, 470
  - editing for Application Engine SSO on WebSphere 461
  - editing for container-managed authentication 458
- WebLogic
  - application server startup script 472
  - configuring Application Engine 144
  - configuring Application Engine
    - upgrade 470, 474
  - configuring application server files 146
  - deploying Application Engine 156, 157
  - deploying Application Engine
    - upgrade 483, 484
- WebLogic 9.2 475
- WebSphere
  - configuring Application Engine 132
  - configuring Application Engine
    - upgrade 458
  - deploying Application Engine 153
  - deploying Application Engine
    - upgrade 478, 479
- workflow subscription wizard 163
- Workplace 145
  - Application Integration collocation issues 184
  - configuring SSL access to 171
  - defining workflow features for users 174
  - deploying a second instance 189
  - deploying additional instances as an EAR file 190
  - designing publishing templates for users 174
  - designing searches for users 174
  - enable access to tasks and work items 167

- Workplace (*continued*)
  - enable for access to IS documents 191
  - enabling for access to IS documents
    - upgrade 494
  - installing Application Integration 184
  - installing File Tracker 186
  - setting bootstrap properties 159
  - setting documentation server URL 160
  - specifying Application Engine administrators 160
  - upgrading Application Integration 487, 488
  - upgrading File Tracker 487, 489
- Workplace Application Integration
  - removing 525
  - removing interactively 525
  - removing silently 525
- Workplace File Tracker
  - removing 527
  - removing interactively 527
  - removing silently 527







Program Number: 5724-R76  
5724-R81

GC19-2802-01

