IBM FileNet P8 Platform
Version 4.5.1

Installation Guide
for installation Solaris with IBM DB2
for Linux, UNIX, and Windows, IBM
WebSphere Application Server, and
IBM Tivoli Directory Server

IBM ®

IBM FileNet P8 Platform
Version 4.5.1

Installation Guide
for installation Solaris with IBM DB2
for Linux, UNIX, and Windows, IBM
WebSphere Application Server, and
IBM Tivoli Directory Server

IBM ®

Contents

ibm.com and related resources

Product support and documentation are available from 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 viii
To contact IBM customer service in the United States or Canada, call 1-800-IBM-SERV (1-800-426-7378).

How to send your comments

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

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

Consumability survey

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

Contacting IBM

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

To learn about available service options, call one of the following numbers:
* In the United States: 1-888-426-4343
* In Canada: 1-800-465-9600

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

Part 1. Installing 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 9
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 63
This topic explains how to install and configure Content Search Engine.

"Installing and configuring Process Engine" on page 81
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 95
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 123
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 135
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 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 5
   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 7

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 8
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).

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.

- 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.

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	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.

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 7.

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/IndexOld` 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.

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
UNIX®	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.

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	http://*yourdocserver*:9080/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.

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.

1. "Installing Content Engine and related client software" on page 10
   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 18
   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 42
   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 48
   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 51
   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 52
   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 54
   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 55
   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 60
   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 62
    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"
   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 13
   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 14
   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 14
   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 16
   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 installContent 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 installContent 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"
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" on page 12
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
Solaris	P8CE-4.5.1-SOL.BIN

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
Solaris	`P8CE-4.5.1-SOL.BIN -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	1. Run the following command in the software package: `P8CE-4.5.1-WIN.exe`. 2. Complete the installation program wizard.
To install silently	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"
   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
Solaris	P8CSE-CLIENT-4.5.1-SOL.BIN

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:
   - 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`

4. Start the Content Search Engine Client installation program.

Operating System	Installation Program
Solaris	`P8CSE-CLIENT-4.5.1-SOL.BIN —f CSEClient_silent_install.txt —i silent`

5. Review the following Content Search Engine Client log files:
   - 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 17
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
Solaris	`P8PE-CLIENT-PE_version-SOL.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
Solaris	`P8PE-CLIENT-PE_version-SOL.BIN -silent -options "PEClient_silent_install.txt"`

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 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"
   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 20
   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`

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 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" on page 21
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 28
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"
   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 22
   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 22
   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 23
   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 24
   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 25
   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 26
   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: `ce_install_path/tools/configure/configmgr`

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 174.

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 180
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.

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 180
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.

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 180
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**.

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.

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 180
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 180
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 33
   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 36
   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 40
   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 configurejdbcgos.xml configurejdbcos.*n*.xml , where *n* is an integer starting with 2	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 59. 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 configureldap.*n*.xml , where *n* is an integer starting with 2	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.
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 31
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
   ```
   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 managedWebSphere 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.

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_cl storepasswords [-task task_type | -taskfile task_file_name]
       -profile myprofile
      ```
      where:

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

Table 6. task_type values

Task	Configuration file	Description

omitted	`applicationserver.xml`
	
	`configurebootstrap.xml`
	
	`configurejdbc.xml`
	
	`configureldap.xml`
	
	`deployapplication.xml`
		When you omit the **-task** *task_type* parameter, you are prompted to enter the passwords for each configuration XML file in the profile. Each password is encrypted before it is added to the XML file.

configurebootstrap	`configurebootstrap.xml`	Encrypts the password for the `BootstrapPassword` property that is used to create the Global Configuration Data and to start Content Engine.
configurejdbcgcd	`configurejdbcgcd.xml`	Encrypts the password for the `DatabasePassword` property that Content Engine uses to access the GCD database.
configurejdbcos	`configurejdbcos.xml` `configurejdbcos.n.xml`, where *n* 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.n.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 177 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.

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 `<TaskEnbled>` element set to false is
   skipped.
   "Running one configuration XML file at a time" on page 37
   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 `<TaskEnbled>` 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.

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 177 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.
- 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 41
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 41 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 18 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:

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

  "Deploying instances by using the graphical user interface"
  You can deploy a Content 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 44
  From the command line you can deploy the Content Engine application on the application server.

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:
	
	`ce_install_path/tools/configure/`
	`configmgr`
	
	where *ce_install_path* 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 180
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"
   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 46
   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 47
   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 47
   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 a 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 is 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 18, 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.

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 or updating EMC Centera SDK library files" on page 49
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 49
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 49
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.

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`

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 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 50
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
Solaris	/opt/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

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.

Option	Description
UNIX	install.sh

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.

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

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

Solaris	From:
	
	``CENTERA_LIB_PATH=/opt/Centera_SDK/lib/32
	LD_LIBRARY_PATH=$LD_LIBRARY_PATH:
	  $CENTERA_LIB_PATH
	export LD_LIBRARY_PATH```
	
	to:
	
	``CENTERA_LIB_PATH=
	install_path /lib/32
	LD_LIBRARY_PATH=$LD_LIBRARY_PATH:
	  $CENTERA_LIB_PATH
	export LD_LIBRARY_PATH```
	
	or:
	
	``CENTERA_LIB_PATH=install_path /lib/64
	LD_LIBRARY_PATH=$LD_LIBRARY_PATH:
	  $CENTERA_LIB_PATH
	export LD_LIBRARY_PATH```

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

Application Server	Startup Script (UNIX)	Startup Script (Windows)
WebSphere Application Server	`setupCmdLine.sh`	`setupCmdLine.cmd`

4. 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)"
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)

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
Stand-alone server	Stop and start the application server.
Network Deployment	Stop and start the application server where Content Engine is deployed, including the Deployment Manager and all managed nodes.
Cluster	Stop and start the cluster.

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 8. Example FileNet P8 System Health page address

Application Server Type	Web Page Address
IBM WebSphere Application Server	`http://`*server*`:9080/P8CE/Health`

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 9. FileNet P8 System Health page contents

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

3. Optional: Bookmark the FileNet P8 System Health page Web page address in your browser for later use.
4. Browse to the 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 10. Example FileNet Engine Web page address

Application Server Type	Web Page Address
IBM WebSphere Application Server	http://myserver:9080/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	*WAS_install_path*/AppServer/profiles/ *profile_name*/logs/*server_name*/ SystemOut.log

   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 57
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 59
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 11. Required application server state

Option	Description
WebSphere Application 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.

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 22
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 180
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 12. Required application server state

Option	Description
WebSphere Application 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. 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 180
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 59 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 14.
- Create XA and non-XA data sources for the object store, as indicated in "Creating the data sources for an object store" on page 55).
- 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 68
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 72
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 74
Use this procedure to configure the storage location and related security for your K2 collections.

"Configuring Content Engine for content-based retrieval" on page 76
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 78
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"
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 64
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.

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 to 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 66
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 67
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
Solaris	P8CSE-4.5.1.0-SOL.BIN

5. Complete the installation program screens by using the values in your worksheet.

6. 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.

7. 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.

   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
   ```

8. Access the host machine and log on as a user with root privileges.

9. 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
Solaris	_ssol26

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
Solaris	`P8CSE-4.5.1.0-SOL.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`.

   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
Solaris	_ssol26

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
Solaris	Start services:
	nohup *verity_install_path*/k2/ _ssol26/bin/k2adminstart &
	Stop services:
	verity_install_path/k2/ _ssol26/bin/k2adminstop

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 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

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:

     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.

   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**.

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.

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 (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
Solaris	*/verity_install_path*/k2/ _ssol26/bin/k2adminstop

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
Solaris	setSolaris.bin

   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
Solaris	nohup *verity_install_path*/k2/ _ssol26/bin/k2adminstart

15. 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

UNIX	1. Open the following K2 configuration file in a text editor:
	
	`verity_install_path`/k2/common/ `verity.cfg`
	
	2. Modify the next available alias settings by adding the collections path. For example, change alias6, mapping6, and dirmode6 to the following:
	
	`alias6=path1`
	`mapping6=/Collections_Directory_Path`
	`dirmode6=wr`
	
	Note: The *Collections_Directory_Path* must be a local path and not a mount point.
	
	3. Save your edits.

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 77 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 88
   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 91
   Start the Process Task Manager and set initial configuration parameters on the Process Engine.

4. "Verifying connection to the Process Engine database" on page 92
   To verify the connection to the Process Engine database, issue the **vwcemp** command.

5. "Installing Process Engine software updates" on page 93
   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 82
   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 83
   Use these procedures to install Process Engine using the installation wizard screens included with the installation package.

3. "Installing Process Engine silently" on page 83
   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 85
   Process Engine installation automatically sets the passwords for several
   internally required local users.
5. "Verifying the connection to the Process Engine database" on page 86
   Verify the ability to connect to the Process Engine database after installing the
   software.
6. "Completing post-installation steps on UNIX platforms" on page 87
   There are additional steps required to complete installation of Process Engine
   on all UNIX 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 (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.

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:

   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 fnsw 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 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*.

"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 (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. Start the installation program.

Platform	Command
Solaris	P8PE-4.5.1-SOL.BIN

4. 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.

5. 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`

6. 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*.

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 (UNIX)"
Complete the following procedures to silently install Process Engine.

"Encrypting passwords for Process Engine" on page 85
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 (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. 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 85 for information on use of the password encryption tool.

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
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 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.

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.

   - `/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*.

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:
   - `fnencryptutils` - an executable .jar file
   - `RunEncryptApp` - a batch file
2. Run one of the following executable files to start the password application:

Option	Description
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.

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 *fnsw* 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
f_sw	• Database (Oracle, SQL) • OS user for DB2	Has privileges only for database objects created by Process Engine. Used as the Process Engine runtime user.	Execute `Xdbconnect`.
f_maint	• Database (Oracle, SQL) • OS user for DB2	Has DBA privileges. Used for RDBMS maintenance.	Execute `Xdbconnect`.

"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 (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
   ```
2. Initiate the connection to the database. At a command prompt, execute:

   `vwcemp -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 (DB2)" on page 86

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 fnsw 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 88
You must run the **killfnsw** command before starting Process Engine.

"Editing the /etc/inittab file (UNIX)" on page 88
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 88
Create a touch file to force FileNet Image Services to use the IPv4 protocol.

Restoring any custom modifications for root and fnsw 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 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
```

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.

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 FileNet 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.

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 89
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 90
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 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 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
Solaris	P8CE-CLIENT-4.5.1-SOL.BIN

9. Complete the installation program wizard by using the values from your worksheet.

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`

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:

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 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. 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
Solaris	`P8CE-CLIENT-4.5.1-SOL.BIN -f` `path/CEClient.Solaris/` `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`

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 onlyProcess Engine values, filter by **Process Task Manager** in the **Installation or Configuration Program** column.

2. Log on to the Process Engine server as *fnsw*.

3. Start the Process Task Manager, as follows:

Option	Description
UNIX	Enter `vwtaskman` at the command prompt. The terminal should support X Windows and the DISPLAY 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
UNIX	/fnsw/local/logs/TM_daemon/ PEDirectoryServerConnectionDebug.txt

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 123.

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 **vwcemp** 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.

`vwcemp -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...."

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 98
   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 98
   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 100
   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 102
   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 115
   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 118
   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 60 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 97
  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.

3. Access the IBM FileNet P8 Application Engine 4.0.2.0 installation software.
4. Start the installation program.

Platform	Command
Solaris	P8AE-4.0.2.0-SOL.bin

5. Complete the Application Engine installer screens by using the values from your worksheet.
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 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:

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.

3. 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.

4. 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`

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`

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"
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 99
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
Solaris	`P8CE-CLIENT-4.5.1-SOL.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`

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
Solaris	`P8CE-CLIENT-4.5.1-SOL.BIN -f` `path/CEClient.Solaris/` `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`

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.

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
Solaris	P8PE-CLIENT-*PE_version*-SOL.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
Solaris	P8PE-CLIENT-*PE_version*-SOL.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"
After you install the Application Engine server, you must configure WebSphere Application Server to work with Application Engine. You can also configure changes for optional modes like SSO.

Configuring Application Engine on WebSphere Application Server

After you install the Application Engine server, you must configure WebSphere Application Server to work with Application Engine. You can also configure changes for optional modes like SSO.

"Editing web.xml for container-managed authentication" on page 103
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 106
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 109
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 111
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 112
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 113
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.

   ```
   <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>/vwsoaprouter</url-pattern>
<url-pattern>/Workflows/*</url-pattern>    Move the closing comment tag from
here to the location indicated at the beginning of this example.
</web-resource-collection>
```

4. Locate the section <auth-constraint>, comment the wildcard (*) <role-name> as noted in the file comments.

```
<auth-constraint>
<!-- <role-name>*</role-name> -->
<!-- For WebSphere 6, use
the role-name line below instead of the wildcard role above.
-->

<role-name>All Authenticated</role-name>

<!-- For WebSphere 6, add this
security-role element below the login-config element (below).
 <security-role>
<description>All Authenticated</description>
<role-name>All Authenticated</role-name>
 </security-role>
-->
</auth-constraint>
```

5. Locate the end of the </login-config> element, and add the All Authenticated users role-element after the closing tag.

```
<security-role>
<description>All Authenticated</description>
<role-name>All Authenticated</role-name>
</security-role>
```

6. Search for the first instance of a <security-constraint> tag, and add the following <security-constraint> tag before that tag.

   Important: Enter the information below as single lines without line breaks.

```
<security-constraint>
<web-resource-collection>
<web-resource-name>action</web-resource-name>
<description>Define the non-secured resource</description>
<url-pattern>/P8BPMWSBroker/*</url-pattern>
</web-resource-collection>
</security-constraint>
```

7. At the end of web.xml, comment out the <login-config> element.

```
<!--
<login-config>
<auth-method>FORM</auth-method>
<realm-name>AE Workplace</realm-name>
<form-login-config>
<form-login-page>/ContainerLogin.jsp</form-login-page>
<form-error-page>/ContainerError.jsp</form-error-page>
</form-login-config>
</login-config>
-->
```

8. As needed, set the *ssoProxyContextPath*, *ssoProxyHost*, *ssoProxyPort*, and *ssoProxySSLPort*.

   These parameter values are used to modify one or more elements of the native URL that Workplace sees on a request. Wherever the value of an SSO proxy host element in the URL request is different from the equivalent information for the host where Workplace is deployed, you must set the corresponding SSO *<proxy host element>* parameter for that element in the URL to the value for the SSO proxy host.

   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 →** *server_name* **→ Java & Process Management → Process Definition → Java Virtual Machine**
WebSphere Application Server 7.0	**Servers → Server Types → WebSphere application servers →** *server_name* **→ Java & Process Management → Process Definition → Java Virtual Machine**

3. In the **Generic JVM arguments** field, add the following entry:

   ```
   -Djava.security.auth.login.config=AE_install_path
   \CE_API\config\jaas.conf.WebSphere
   ```

   Replace *AE_install_path* in the entry above with your actual installation path, such as:

   UNIX: `opt/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.

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	1. Navigate to **Security > Secure administration, applications, and infrastructure**. 2. From the right side of the panel, select **Authentication Mechanisms and expiration**.
WebSphere Application Server 7.0	1. Navigate to **Security > Global security**. 2. From the right side of the panel, select **LTPA**.

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	1. Navigate to **Security > Secure administration, applications, and infrastructure**. 2. From the right side of the panel, select **Authentication Mechanisms and expiration**.
WebSphere Application Server 7.0	1. Navigate to **Security > Global security**. 2. From the right side of the panel, select **LTPA**.

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 **Security > Secure administration, applications, and infrastructure**.
WebSphere Application Server 7.0	Navigate to **Security > Global security**.

3. Disable security by using the following Security settings:
   - Disable (clear) the **Enable Administrative Security** flag.
   - Disable (clear) the **Enable application security** flag.
   - Disable (clear) the **Java 2 security** flag.
4. From the bottom of the panel, in the dropdown list called **Available realm definitions**, select **Standalone LDAP registry** and click **Configure**.

5. Configure the LDAP provider to exactly match the corresponding settings on the Content Engine application server.

   Tip: Open the WebSphere administrative console for Content Engine to the same panels to see and copy all settings.
   - Primary administrative user name
   - Select Automatically generated server identity.
   - Type
   - Host
   - Port
   - Base distinguished name (DN)
   - Bind distinguished name (DN)
   - Bind password
6. Configure the LDAP user registry settings to exactly match the corresponding settings on the Content Engine application server.

   Tip: Open the WebSphere administrative console for Content Engine to the same panel to see and copy all settings.
   - User filter
   - Group filter
   - User ID map
   - Group member ID map
   - Certificate map mode
   - Certificate filter
7. Save these settings.
8. Next to **Available realm definitions**, ensure that **Standalone LDAP registry** is still selected, and click **Set as current**.
9. Set the following Security flags:
   - Enable (select) the **Enable Administrative Security** flag.
   - Enable (select) the **Enable application security** flag.
   - Disable (clear) the **Java 2 security** flag.

   The IBM FileNet P8 Platform utilizes LDAP-based security, and does not support Java 2 security. Enabling Java 2 security will cause unexpected behavior.
10. Save your changes to the master configuration.
11. Restart the WebSphere instance.
12. Test the connection on the Standalone LDAP registry page. If the test fails, correct the error before proceeding. If it passes, click **OK** to return to the previous page.

Configuring Lightweight Directory Access Protocol (LDAP) for federated repositories

If you have a multiple domain environment, configure LDAP settings for federated repositories on the WebSphere Application Server to enable LDAP communication between Application Engine and Content Engine.

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 **Security > Secure administration, applications, and infrastructure**.
WebSphere Application Server 7.0	Navigate to **Security > Global security**.

3. Set the following Security flags:
   - Disable (clear) the **Enable Administrative Security** flag.
   - Disable (clear) the **Enable application security** flag.
   - Disable (clear) the **Java 2 security** flag.
4. From the bottom of the panel, in the dropdown list called **Available realm definitions**, select **Federated Repositories** and click **Configure**.
5. Configure the LDAP provider to exactly match the corresponding **General Properties** on the Content Engine application server.

   Tip: Open the WebSphere administrative console for Content Engine to the same panels to see and copy all settings.
   - Realm name
   - Primary administrative user name
   - Select Automatically generated server identity.
   - Ignore case for authorization
   - Repositories in the realm
6. Save these settings.
7. Next to **Available realm definitions**, ensure that **Federated repositories** is still selected, and click **Set as current**.
8. Set the following Security flags:
   - Enable (select) the **Enable Administrative Security** flag.
   - Enable (select) the **Enable application security** flag.
   - Disable (clear) the **Java 2 security** flag.

   The IBM FileNet P8 Platform utilizes LDAP-based security, and does not support Java 2 security. Enabling Java 2 security causes unexpected behavior.
9. Save your changes to the master configuration.
10. Restart the WebSphere instance.
11. Test the connection to the repository.
    a. In the WebSphere administrative console, navigate to **Users and Groups** → **Manage Users**.
    b. Click **Search By User ID**, and enter a known user.
    c. Click **Search**. This should return the user from the configured LDAP repository.

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 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 116
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 117
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

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`

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.

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 119
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 121

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 122
To allow users to create workflows subscriptions, you must configure the PWDesigner access role using the Workplace Site Preferences, and give the users appropriate access rights to the workflow subscriptions classes.

"Enhanced Timezone Detection" on page 122
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 128 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 13. 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 141.

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 124
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 125
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 126
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 128
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 131
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 125 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 91.

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 91.

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 54
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 123, 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 54
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 127
  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.

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.

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 (defautl) While the default port for IIOP with SSL is port 9403, use port 2809. The web application server resolves the SSL port number correctly.

The port values in the table are default values. If you change the port that your application server listens on, you might need to change the port number used by the Content 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"
  To set up full SSL support, enable SSL on the preferred application server.

  "Setting up SSL redirect on a single Application Engine server"
  To set up SSL redirect, enable SSL on the preferred application server, set your bootstrap preferences, update the base URL, and sign out.

  "Setting up SSL redirect on two Application Engine servers" on page 130
  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 131
  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 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 ecm_help documentation package	http://*yourdocserver:port*#/ecm_help/ _start_here.htm

- 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.

"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.

"Creating additional file storage areas" on page 138
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**.

"Deploying multiple Application Engine instances" on page 139
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 141
Image Services Resource Adaptor (ISRA) is a J2EE connector to the IBM FileNet Image Services libraries. Using ISRA, Workplace users can view FileNet Image Services documents and their associated annotations in the FileNet Image Viewer and, if they have the appropriate permissions, update the annotations.

"Installing and configuring IBM System Dashboard for Enterprise Content Management" on page 145
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 145
You can add Autonomy K2 servers or move existing servers to new hardware.

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 91), 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 123.

4. Right-click the **CE_Operations** component queue and select **Properties** .

5. 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.

6. 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 137
   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.

1. 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

   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 `vwtaskman.xml` will not be automatically created. If this happens, make a copy of the sample `vwtaskman.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:
-
  - `/opt/FileNet/AE/Router` on UNIX

Open `vwtaskman.xml.sample` with a text editor, change the port element value to an available port number, and save the file to `vwtaskman.xml` in the same directory.

2. In Process Task Manager, select the server name in the left pane.
3. Find the Registry Port for the server in the right pane and verify that it is correct.
4. Select **Component Managers** in the left pane .
5. 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.
6. 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

�邑 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: `vwtaskman`

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.

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*.

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 140
You can choose to deploy your additional application instance as an EAR file.
You must perform the additional configuration for each custom Workplace
instance you plan to deploy.

Deploying a second instance of Workplace

Each deployment of Workplace might use different Site Preference settings and
might provide access to different object stores.

To deploy a second instance of the Workplace application:

1. Make a copy of the `/FileNet/Config/AE` directory, including all of its contents,
   for each instance you plan to deploy. For example, if you are deploying two
   instances, you would create:

   install_path/FileNet/Config/AE1

   install_path/FileNet/Config/AE2

2. Make copies of the upload and download directories in the
   install_path/FileNet/AE directory. For example, you would create:

   install_path/FileNet/AE/Download1

install_path/FileNet/AE/Upload1

install_path/FileNet/AE/Download2

install_path/FileNet/AE/Upload2

3. Make a copy of the deploy directory and all of its contents for each Workplace instance. For example, you would create:

   install_path/FileNet/AE/deploy1

   install_path/FileNet/AE/deploy2

4. Make a copy the Workplace directory and all of its contents for each Workplace instance. For example, you would create:

   install_path/FileNet/AE/Workplace1

   install_path/FileNet/AE/Workplace2

5. Navigate to each custom copied Workplace web.xml instance and update the path for the configuration directory, upload directory, and download directory locations.

   For example, in the *install_path*/FileNet/AE/Workplace1/WEB-INF/web.xml, you would make the following changes:

   ```
    <context-param>
     <param-name>configurationDirectory</param-name>
     <param-value>/opt/FileNet/Config/AE1</param-value>
   </context-param>

    <context-param>
     <param-name>uploadDir</param-name>
     <param-value>/opt/FileNet/AE/Upload1</param-value>
   </context-param>
   <context-param>
     <param-name>downloadDir</param-name>
     <param-value>/opt/FileNet/AE/Download1</param-value>
   </context-param>
   ```

Deploying each additional Workplace instance as an EAR file

You can choose to deploy your additional application instance as an EAR file. You must perform the additional configuration for each custom Workplace instance you plan to deploy.

1. Modify the application.xml file located in the copied deploy directories, as follows:

   a. Open each instance of the application.xml file, for example, *install_path*/FileNet/AE/deploy1/META-INF/application.xml.

   b. Change the <display-name> and the <context-root> elements to your custom name, for example, Workplace1 (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 FileNet Image Services documents and their associated annotations in the FileNet Image Viewer and, if they have the appropriate permissions, update the annotations.

To enable Workplace users to view documents by using ISRA:

- Install Application Engine.
- Install FileNet Image Services Resource Adaptor.

  For information on installing, configuring and deploying FileNet ISRA, See the Image Services Resource Adapter documentation in the FileNet ISRA installation package.

  Tip: Use the Sample Application shipped with FileNet ISRA to confirm that the ISRA installation was successful.

  Important: In an ISRA upgrade situation, take care to use the same library name (JNDI connection factory name) that has been previously set in the ISRA installation. Changing this variable can cause conflicts when accessing documents.

- Install the Application Engine ISRA Servlet and take the following into account:
  - Install and deploy ISRA before installing and deploying the ISRA Servlet.
  - Deploy the ISRA Servlet on the same application server as FileNet ISRA.
  - It is not necessary to install the ISRA Servlet on the Application Engine server. See "ISRA SSL support" on page 142 for details that might affect your collocation plans.

- Configure Workplace Site Preferences.

  "ISRA SSL support" on page 142
  The following table details supported SSL configurations for ISRA.

  "Installing and deploying the Application Engine ISRA servlet" on page 142
  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 144
Before using the ISRA servlet, you must enable the FileNet Image Services external service and set the ISRA Interface Servlet URL in Workplace Site Preferences.

"Logging in to FileNet Image Services by using an LDAP account" on page 144
In order to log in to FileNet Image Services by using your LDAP account, you must configure ISRA for LDAP authentication.

"Accessing FileNet Image Services library documents" on page 145
For information about accessing FileNet 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.

2. 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.

3. Stop the application server if it is running.
4. Access the ISRA installation package, and start the following Application Engine ISRA Servlet setup program, depending on your operating system:

Option	Description
UNIX	AE-ISRA-Servlet-4.0.2.0- *operating_system*.bin

5. Complete the installation program screens by using the values from your worksheet.
6. Check the file AE_ISRA_Servlet_install_log-4_0_2_0.txt, located in the *AE_israservlet_install_path*\FileNet directory, to see if any errors occurred during the installation.
7. Install unlimited strength JAR files.

   Perform this step only if the following are true:

   - You selected the option to create Strong keys in the Application Engine User Token Security step of the Application Engine installation.
   - Application Engine ISRA Servlet is deployed on a different application server than Application Engine.

   Important: If these conditions are true, failure to perform this step causes an EncryptionException when you log on to the IS server.
8. (WebSphere Application Server and WebLogic Server only) Start the application server.
9. Deploy *AE_israservlet_install_path*/FileNet/ ApplicationEngineISRAServlet/ae_isra.war in the same way you deployed the app_engine.war file for Workplace.
10. Verify the Application Engine ISRA Servlet is installed and deployed correctly, as follows. This step launches a diagnostic tool that does the verification.

    a. Open your web browser.
    b. Enter the URL for the Application Engine ISRA Servlet, for example:

       http://*ApplicationEngineISRAServlet_servername:port*/ ApplicationEngineISRAServlet/ISRA

    ApplicationEngineISRAServlet is the default context root. If you specified a different name for the context root when deploying the Application Engine ISRA Servlet, change the URL to match your configuration.

    If the ISRA Servlet is set up correctly, a congratulations message displays, for example:

```
Congratulations! ISRA Interface Servlet is configured at this URL.

WcmApiConfigFile = D:\ISRAInterface\jsp\WEB-INF\WcmApiConfig.properties

WcmApiConfig file exists

CryptoKeyFile/UserToken = C:\Program
Files\FileNet\Authentication\UTCryptoKeyFile.properties

CryptoKeyFile/UserToken exists


FileNet ISRA classes are in the classpath

com.filenet.is.ra.cci.FN_IS_CciConnectionSpec
```

Configuring Workplace site preferences for ISRA

Before using the ISRA servlet, you must enable the FileNet Image Services external service and set the ISRA Interface Servlet URL in Workplace Site Preferences.

The Application Engine installation program installs the pre-configured Image Services external service, which includes the parameterized values necessary to access FileNet IS libraries from Workplace.

To configure Workplace Site Preferences for ISRA Servlet support:

1. Sign in to Workplace as a user having the Application Engine Administrators access role.
2. Launch Site Preferences as follows:
   a. Select **Admin**.
   b. Select **Site Preferences**.
3. Enable the pre-configured Image Services external service, as follows:
   a. Select **External Services** from the left options list.
   b. Select **Modify** for the Image Service, located under External Reference Services.

      The External Reference Service Settings site preference page displays.
   c. Under General Information, locate **Show on Select File page** and change the value to Show.
   d. Accept the setting.
4. Set the ISRA Interface Servlet URL as follows:
   a. Select **Bootstrap**.
   b. Under Preferences Settings, set the value of ISRA Interface Servlet URL. For example:

      http://*servername*:*port*/ApplicationEngineISRAServlet/ISRA

      ApplicationEngineISRAServlet is the default context root. If you specified a different name for the context root when deploying the Application Engine ISRA Servlet, change the URL to match your configuration.
   c. Accept the setting.
   d. Exit Site Preferences.

Logging in to FileNet Image Services by using an LDAP account

In order to log in to FileNet Image Services by using your LDAP account, you must configure ISRA for LDAP authentication.

To log in to the FileNet Image Services library by using your LDAP account:

1. Configure ISRA for LDAP authentication.

   For information on configuring LDAP authentication for ISRA, See the *ISRA Installation and Deployment Guide*. For information on configuring LDAP authentication for FileNet Image Services, See the *Image Services System Tools Reference Manual*.

2. Configure FileNet Image Services for LDAP authentication.

   If the LDAP account with which you accessed Workplace is not valid for the FileNet Image Services library, or if LDAP authentication is not configured, you will be prompted to log in to the FileNet Image Services library.

Accessing FileNet Image Services library documents

For information about accessing FileNet Image Services library documents, see **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 149
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 148
You can start or stop the Autonomy K2 services using manual commands, according to your environment.

"Configuring additional K2 administration servers" on page 148
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 15. Directory by platform

Platform	Directory
Solaris	_ssol26

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.

   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. 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)"
   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 148
   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
Solaris	P8CSE-4.5.1.0-SOL.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 16. Silent installation commands by platform

Platform	Command
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`.

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 (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

Solaris	Start services:
	`nohup verity_install_path`
	`/k2/_ssol26/bin/k2adminstart &`
	
	Stop services:
	`verity_install_path`
	`/k2/_ssol26/bin/k2adminstop`

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 150
   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 74.

      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.

Part 2. 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

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 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 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.

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 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 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"
In silent mode, the uninstaller removes all Content Engine components.

"Removing data associated with Content Engine"
After uninstalling Content Engine, you can remove its associated data.

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	ce_uninstaller -i silent

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.
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. User 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
UNIX	1. Stop the Autonomy K2 Administration Server service and the Tomcat application server. Use the following command, according to your environment:
	Solaris *verity_install_path*/k2/ _ssol26/bin/k2adminstop
	2. Change directory to: *verity_install_path*/_cseuninst
	3. Run the following command: ./CSE_uninstaller

6. Delete *verity_install_path* on the machine.
7. Repeat 5 on page 157 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 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:

   `killfnsw -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.

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 whereApplication Engine is installed.

2. Log in to the WebSphere administrative console.
3. Uninstall the Workplace application.
   a. Stop the Workplace process in the admin console.
   b. Uninstall the Workplace application from Enterprise Applications.
4. Navigate to the /_uninst folder under the Application Engine installation location.
5. Run the uninstall program:

Option	Description
UNIX	uninstaller.bin

6. Delete the Workplace folder: *WAS_HOME*/temp/*node_name*/*application_server_name*/Workplace
7. Delete the *AE_install_path* directory.
8. (If Application Engine is the only IBM FileNet P8 application installed on the server) Search for the vpd.properties file. If it exists, delete it.

   Important: In the following step, do not remove the system environment variable if any other IBM FileNet P8 application is installed on the server.

9. (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 the Application Engine ISRA servlet

Removal of the Application Engine ISRA Servlet for Windows and UNIX environments requires that you logon to the application server, undeploy the servlet, and run the uninstall program.

Since the installed names for the ISRA Servlet are configurable on the supported application servers, the following information might not be the same as your environment. Make the appropriate name changes as required for your environment.

To remove the Application Engine Servlet software:

1. Log on to the application server.

Option	Description
UNIX	Log on as a user with write access to the directory where ISRA Servlet is installed.

2. Undeploy the ApplicationEngineISRAServlet application. This step is similar to that required to undeploy the Workplace application.

Option	Description
IBM WebSphere Application Server	1. Stop the ApplicationEngineISRAServlet process in the Admin console. 2. Uninstall the ApplicationEngineISRAServlet application from Enterprise Applications.

3. Navigate to the /_uninstISRA directory under the ISRA Servlet installation location.
4. Run the uninstall program:

Option	Description
UNIX	uninstall.bin

5. Navigate to the /FileNet directory. If there is no other FileNet software installed under this directory, delete the /FileNet directory. If there is some other FileNet software installed under this directory, delete only the /ApplicationEngineISRAServlet subdirectory.
6. (WebSphere Application Server only) Delete the following temporary working folders for the Application Engine ISRA Servlet: *WAS_Home*\WebSphere\ AppServer\profiles\default\installedApps*servername*\ ApplicationEngineISRAServlet.ear\

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 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.

Part 3. 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 174
  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 177
  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 177
  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 178
  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 179
  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 180
  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 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.

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.

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 188 or "Editing the application server properties" on page 189 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 the 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 190 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 191 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 191 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 191 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 191 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 195.
- **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 188 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 195.

- 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 195. For more information about checking the task status from the CLI, see "Running Configuration Manager commands" on page 197.

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	*WAS-Home*/AppServer/bin/ikeyman.sh

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 178. For example, the File Name filed 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 178.

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 197.

"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 181
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 184
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 186
You can use the Configuration Manager commands, icons, and panes to work with your profiles and configuration tasks.

"configmgr.ini parameters" on page 196
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: *ce_install_path*/tools/configure/configmgr

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"
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 182
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 182
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 183
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
	New Installation Profile
	Click this icon to create a profile for a new installation. The current configuration profile will be closed, and the New Configuration Profile Wizard starts. If the existing open profile has been changed, you will be prompted to save your changes.
	New Upgrade Profile
	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.
	Open Profile
	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.
	Save
	Click this icon to save the current configuration profile settings.
	View Configuration Manager Log File
	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.

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
	Edit Application Server Properties
	Click this icon to view or edit the application server properties for the current profile.
	Run All Tasks
	Click this icon to run all the enabled tasks for the current profile.

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
	Enable the Selected Task Click this icon to enable a task. The Run All Tasks command only runs tasks that are enabled.
	Disable the Selected Task Click this icon to disable a task. The Run All Tasks command only runs tasks that are enabled.
	Save Click this icon to save the current task.
Test Database Connection	Test Database Connection 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.
Test LDAP Connection	Test LDAP Connection Configure LDAP task tab only. Click this button to test the connection to the directory service provider by using the values provided.

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
	Clear Console 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.
	Scroll Lock 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.
	Pin Console 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.

Icon	Command name and Description
	Display Selected Console Click this icon to select the console tab to display. Select the desired tab from the list of recently viewed consoles.
	Open Console 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.

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 17. 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 188 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 188 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
	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

Table 17. Main Menu Commands (continued)

Menu name	Command name	Description
	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 18. 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.
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 19. Task Icon Pop-Up Menu Commands

Command	Description
Edit Selected Task	Opens the task in the task pane for editing.

Table 19. Task Icon Pop-Up Menu Commands (continued)

Command	Description
Enable Selected Task Disable Selected Task	Toggles the state of the task between enabled and disabled. Any task that is disabled will not run with either the **Run Selected Task** command or the Run All Tasks command. If the task is currently enabled, selecting the **Disable Selected Task** command prevents the task from running, changes the font for the task icon to italic, and appends "(disabled)" to the icon label. If the task is currently disabled, selecting the **Enable Selected Task** command allows the task to run, restores the original font, and removes "(disabled)" from the icon label.
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 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 187
You can use the Configuration Manager graphical user interface to configure a Content Engine instance.

"Setting the password save preference" on page 188
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 188
You must create a new configuration profile for each Content Engine
application that you deploy.

"Opening and closing an existing profile or task" on page 189
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 189
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 190
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 192
You must run a task to apply the values that you provided.

"Adding an additional task to your profile" on page 194
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 194
You can delete any unneeded tasks from your profile.

"Running all tasks at the same time" on page 195
You can run all the tasks in a profile at the same time. Disabled tasks will not
run.

"Running a single task" on page 195
You can run each configuration task individually. Disabled tasks will not run.

"Checking the task status" on page 195
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 196
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 196
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" on
   page 188.
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 190
   - "Editing the configure LDAP task" on page 191
   - "Configuring the login modules" on page 192

- "Editing the configure bootstrap properties settings" on page 191
3. Apply the configuration settings by running the tasks. See "Running all tasks at the same time" on page 195.
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 191.

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 **Save all passwords to file when saving a task or profile** check box.
To prevent writing passwords to file	Clear the **Save all passwords to file when saving a task or profile** check box.

3. Click **OK**.

Creating a profile for a new installation

You must create a new configuration profile for each Content 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 panewith 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)

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 theses 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"
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" on page 191
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 191
The bootstrap information is needed for creating the Global Configuration Data and for starting Content Engine.

"Editing the deploy application task" on page 191
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 **Create New**.
To modify an existing deployed EAR file	Select **Modify Existing**.
To upgrade an existing deployed EAR file	Select **Upgrade**.

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 18
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"
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 193
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 193
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 193
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 177.

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 177.

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.

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	`ce_install_path/tools/configure/configmgr_cl`

"How to read the syntax diagrams" on page 198
Syntax diagrams describe how you must enter commands and what options are available.

"**checkstatus** command" on page 198
The **checkstatus** command checks the status of the specified configuration task. The command name is not case sensitive.

"**execute** command" on page 202
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 206
The **generateconfig** command generates the configuration XML file for the specified configuration task. The command name is not case sensitive.

"**gui** command" on page 211
The **gui** command opens the Configuration Manager graphical user interface. The command is not case sensitive.

"**listtasks** command" on page 212
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 215
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 218
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 221
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 20. task_type values

Option	Configuration file	Description

omitted	`configurebootstrap.xml`
	
	`configurebootstrap.n.xml`
	
	`configurejdbcgcd.xml`
	
	`configurejdbcos.xml`
	
	`configurejdbcos.n.xml`
	
	`configureldap.xml`
	
	`configureldap.n.xml`
	
	`configureloginmodules.xml`
	
	`deployapplication.xml`
	
	Where *n* is an integer starting with 2
		If you omit the **-task** *task_type* parameter and the **-taskfile** *task_file_name* parameter, then the status for all the configuration files in the profile is displayed.

`configurebootstrap`	`configurebootstrap.xml` `configurebootstrap.n.xml`, where *n* 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 `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 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 `configurebootstrap` task, then you must specify the **-taskfile** *task_file_name* 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 20. task_type values (continued)

Option	Configuration file	Description
configurejdbcos	configurejdbcos.xml configurejdbcos.*n*.xml, where *n* is an integer starting with 2	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. 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. If your profile contains more than one configurejdbcos task, then you must specify the **-taskfile** *task_file_name* parameter to identify the task to check.
configureLDAP	configureldap.xml configureldap.*n*.xml, where *n* is an integer starting with 2	Checks status for configuring 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 cannot change the filename, but you can edit the value in the file for the name of the task. If your profile contains more than one ConfigureLDAP task, then you must specify the **-taskfile** *task_file_name* parameter to identify the task to check.

Table 20. 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 configurejbcos -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 is 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 21. task_name values

Option	Configuration file to execute	Description
omitted	configurebootstrap.xml	If you omit the **-task** *task_type* parameter and the **-taskfile** *task_file_name* parameter, then all the configuration files in the path are run. Any configuration XML file that has the **enabled** attribute value in the **<configuration>** tag set to false is skipped.
	configurebootstrap.*n*.xml	
	configurejdbcgcd.xml	
	configurejdbcos.xml	
	configurejdbcos.*n*.xml	
	configureldap.xml	
	configureldap.*n*.xml	
	configureloginmodules.xml	
	deployapplication.xml	
	where *n* is an integer starting with 2	

Table 21. task_name values (continued)

Option	Configuration file to execute	Description
configurebootstrap	configurebootstrap.xml configurebootstrap.*n*.xml, where *n* is an integer starting with 2	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 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. If your profile contains more than one configurebootstrap task, then you must specify the **-taskfile** *task_file_name* parameter to identify the task to run.
configurejdbcgcd	configurejdbcgcd.xml	Applies the settings for configuring the JDBC connections to the Global Configuration Data (GCD) database used by Content Engine.

Table 21. task_name values (continued)

Option	Configuration file to execute	Description
`configurejdbcos`	`configurejdbcos.xml` `configurejdbcos.n.xml`, where *n* is an integer starting with 2	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. When you generate a second object store JDBC configuration file, it is named `configurejdbcos.2.xml`. The filename increments for each new file you generate. You can edit the file name as needed. If your profile contains more than one `configurejdbcos` task, then you must specify the **-taskfile** *task_file_name* parameter to identify the task to run.
`configureldap`	`configureldap.xml` `configureldap.n.xml`, where *n* 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. If your profile contains more than one `configureldap` task, then you must specify the **-taskfile** *task_file_name* parameter to identify the task to run.
`configureloginmodules`	`configureloginmodules.xml`	(WebSphere Application Server or JBoss Application Server only.) Creates the login modules for the Content 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.

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 22. task_type values

Option	Configuration file to generate	Description
omitted	`applicationserver.xml`	If you omit the `-task` *task_type* parameter and the **-taskfile** *task_file_name* parameter, then all the default configuration files for a profile are created.
	`configurebootstrap.xml`	
	`configurejdbcgcd.xml`	
	`configurejdbcos.xml`	
	`configureldap.xml`	
	`configureloginmodules.xml`	
	`deployapplication.xml`	

Table 22. task_type values (continued)

Option	Configuration file to generate	Description
configurebootstrap	applicationserver.xml configurebootstrap.xml configurebootstrap.*n*.xml, where *n* is an integer starting with 2	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 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 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. If the profile already contains an applicationserver.xml file, the existing file is retained.
configurejdbcgcd	applicationserver.xml configurejdbcgcd.xml	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. If the profile already contains an applicationserver.xml file, the existing file is retained.

Table 22. task_type values (continued)

Option	Configuration file to generate	Description
configurejdbcos	applicationserver.xml configurejdbcos.xml configurejdbcos.*n*.xml, where *n* is an integer starting with 2	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. 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. If the profile already contains an applicationserver.xml file, the existing file is retained.
configureldap	applicationserver.xml configureldap.xml configureldap.*n*.xml, where *n* is an integer starting with 2	Generates the file for the application server properties and the file 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. You cannot change the filename, but you can edit the value in the file for the name of the task. If the profile already contains an applicationserver.xml file, the existing file is retained.

Table 22. 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.

-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
```

gui command

The **gui** command opens the Configuration Manager graphical user interface. The command is not case sensitive.

gui command syntax

```
configmgr_cl gui
```

gui command Example

The following command starts the Configuration Manager graphical user interface:

```
configmgr_cl gui
```

listtasks command

The **listtasks** command displays a list of the tasks and the task files in the configuration profile. The command name is not case sensitive.

listtasks command syntax

```
configmgr_cl listtasks [-task task_type]  -profile myprofile
 [-help]
```

listtasks command parameters

-task *task_type*

The **-task** *task_type* parameter is optional and indicates which task type to list. The *task_type* value is not case sensitive. The following table lists the valid task names, the associated configuration XML file, and a description of the Content Engine settings affected by the task.

Table 23. task_type values

Option	Configuration files	Description
omitted	configurebootstrap.xml configurebootstrap.*n*.xml configurejdbcgcd.xml configurejdbcos.xml configurejdbcos.*n*.xml configureldap.xml configureldap.*n*.xml configureloginmodules.xml deployapplication.xml Where *n* is an integer starting with 2	If you omit the -task *task_type* parameter, then all the configuration tasks and the associated task files for the profile are listed.
configurebootstrap	configurebootstrap.xml configurebootstrap.*n*.xml, where *n* 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 configurebootstrap.2.xml. The filename increments for each new file you generate.

Table 23. task_type values (continued)

Option	Configuration files	Description
configurejdbcgcd	configurejdbcgcd.xml	Lists the task for configuring the settings for the JDBC connections to the Global Configuration Data (CGD) database used by Content Engine.
configurejdbcos	configurejdbcos.xml configurejdbcos.*n*.xml, where *n* 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.*n*.xml, where *n* 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.
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 24. task_type values

Option	Configuration files	Description
configurebootstrap	configurebootstrap.xml configurebootstrap.*n*.xml, where *n* 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 24. 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.*n*.xml, where *n* 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.*n*.xml, where *n* 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.
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 configureoginmodules -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 25. task_type values

Option	Configuration file to remove	Description
configurebootstrap	configurebootstrap.xml configurebootstrap.*n*.xml, where *n* 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.

Option	Configuration file to remove	Description
configurejdbcos	configurejdbcos.xml configurejdbcos.*n*.xml, where *n* 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.*n*.xml, where *n* 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 **-taskfile** *task_file_name* 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 26. task_type values

Option	Configuration file	Description
omitted	applicationserver.xml	If you omit the **-task** *task_type* parameter and the **-taskfile** *task_file_name* parameter, then you are prompted to enter the passwords for each configuration XML file in the profile. Each password is encrypted before it is added to the XML file.
	configurebootstrap.xml	
	configurebootstrap.*n*.xml	
	configurejdbcgcd.xml	
	configurejdbcos.xml	
	configurejdbcos.*n*.xml	
	configureldap.xml	
	configureldap.*n*.xml	
	deployapplication.xml	
	Where *n* is an integer starting with 2	

Table 26. task_type values (continued)

Option	Configuration file	Description
configurebootstrap	configurebootstrap.xml configurebootstrap.*n*.xml, where *n* 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.*n*.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.*n*.xml, where *n* 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.*n*.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.

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.

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	`/fnsw/local/logs/TM_daemon/` `PEDirectoryServerConnectionDebug.txt`

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 228
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 228
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 229
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	http://myserver:9080/FileNet/Engine

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	`http://CEserver:9080/wsi/FNCEWS40MTOM/`

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 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 ($^{\circledR}$ or $^{\text{™}}$), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml (www.ibm.com/legal/copytrade.shtml).

Java and all Java-based trademarks 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

additional file storage areas 138
AddOn installation problems
  troubleshooting 225
Application Engine
  access roles 119
  administrator access roles 119
  administrators 119
  Application Name 121
  configuring on all application
    servers 102
  configuring on WebSphere 102
  configuring SSL 129
  container-managed authentication on
    WebSphere 103
  deploying on all application
    servers 115
  deploying on WebSphere 115
  deploying on WebSphere 6.1 116
  deploying on WebSphere 7.0 117
  indexing 121
  installing 95
  installing and configuring 95
  installing Content Engine Client 98
  installing interactively 96
  installing silently 97
  installing software updates 98
  multiple instances 139
  removing ISRA servlet 165
  removing on WebSphere 163
  setting up full SSL support 129
Autonomy K2
  installing Content Search Engine 63
  moving administration servers 149
  non-English locales 73
Autonomy K2 administration server
  installing additional interactively
    UNIX 147
  installing additional silently
    UNIX 147
Autonomy K2 administration servers
  UNIX 146
Autonomy K2 server
  modifying configuration 145
Autonomy K2 servers
  moving 149
Autonomy K2 services
  starting and stopping 148
Autonomy K2 services UNIX)
  starting and stopping 68
auxiliary documentation 5

B

banner image
  changing 119
bootstrap 26
bootstrap preferences
  configuring 118
  enhanced time zone 122

bootstrap preferences *(continued)*
  setting on first login 119
  setting the SSL configuration for
    Application Engine 119
bootstrap properties 191
bootstrap.properties file
  sharing between Application
    Engines 130

C

checking the status of a task from the
  command line 40
checking the task status from the
  command line 40, 41
checkstatus command 198
Component Manager 136
configmgr.ini 196
configuration and startup tasks 123
Configuration manager
  overview 173
Configuration Manager
  config_mgr_user permissions 19
  adding an SSL signer to the
    keystore 178, 179
  adding new tasks 194
  applying configuration settings from
    the command line 36, 38
  applying the Configure Bootstrap
    Properties settings 193
  applying the Configure JDBC Data
    Sources settings 192
  applying the values in a task 192
  changing password preference for
    installation 22
  checking the status of a task 196
  checking the status of a task from the
    command line 40
  checking the task status from the
    command line 41
  checkstatus command 198
  command line interface 28
  command-line reference 197
  Configure Bootstrap settings for
    upgrade 26
  configuring Content Engine using the
    graphical user interface 21
  console toolbar 183
  creating a new profile 188
  deploying Content Engine 194
  editing a configuration XML file for
    installation 33
  editing a task 190
  editing the application server
    properties 190
  editing the Configure Bootstrap
    Properties task 191
  editing the Configure JDBC Data
    Sources task 190
  editing the Configure LDAP task 191

Configuration Manager *(continued)*
  editing the Deploy Application
    task 192
  execute command 202
  generateconfig command 206
  generating a configuration XML file
    for installation 31
  generating all of the configuration
    XML files at the same time for
    installation 30
  grant user permissions 19
  graphical user interface and
    command-line interface
    differences 176
  gui command 211
  GUI reference 180
  installation worksheet 176
  listtasks command 212
  logs 177
  main toolbar 182
  menus and commands 184
  movetask command 215
  new profile 22
  opening an existing profile 189
  overview 174
  passwords 177
  profile concepts 174
  profile toolbar 182
  reference 173
  remove task 194
  removetask command 218
  runing configuration XML files for
    installation 36
  running a selected task 195
  running all configuration XML files at
    the same time 36
  running all tasks at the same
    time 195
  running commands 197
  running configuration XML files one
    at a time 38
  saving changes to a task or
    profile 196
  setting password save preference 188
  starting 22
  starting for installation 180
  storepasswords command 221
  task status 196
  task toolbar 182
  viewing the session log 196
  window description 181
  working in the Configuration
    Manager window 181
  working with 186
configuration profile
  adding new tasks 194
  creating a new profile 22
  renaming tasks 194
configuration tasks
  adding 194
  renaming 194

IBM ®